

TABLE OF CONTENTS

TABLE DES MATIÈRES

A. INTRODUCTION

- 1. Title
- 2. Number
- 3. Purpose
- 4. Applicability
- 5. Effective Date

B. REQUIREMENTS

R1 to R5

C. MEASURES

M1 to M5

D. COMPLIANCE

- 1. Compliance Monitoring Process
 - 1.1 Compliance Monitoring Responsibility
 - 1.2 Compliance Monitoring Period and Reset Time Frame
 - 1.3 Data Retention
 - 1.4 Additional Compliance Information
- 2. Levels of Non-Compliance
 - 2.1 Level 1
 - 2.2 Level 2
 - 2.3 Level 3
 - 2.4 Level 4

E. REGIONAL DIFFERENCES

VERSION HISTORY

A. INTRODUCTION

- 1. Titre
- 2. Numéro
- 3. Objet
- 4. Applicabilité
- 5. Date d'entrée en vigueur

B. EXIGENCES

E1 à E5

C. MESURES

M1 à M5

D. CONFORMITÉ

- 1. Processus de vérification de la conformité
 - 1.1 Responsabilité de la vérification de la conformité
 - 1.2 Période de vérification de la conformité et délai de retour en conformité
 - 1.3 Conservation des données
 - 1.4 Autre information sur la conformité
- 2. Niveaux de non-conformité
 - 2.1 Niveau 1
 - 2.2 Niveau 2
 - 2.3 Niveau 3
 - 2.4 Niveau 4

E. DIFFÉRENCES RÉGIONALES

HISTORIQUE DES VERSIONS

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
-----	-----------------	--	-------------------

A. Introduction / Introduction

1.	Title: Cyber Security — Electronic Security Perimeter(s)	1.	Titre : Cybersécurité — Périmètre(s) de sécurité électronique(s)
2.	Number: CIP-005-1	2.	Numéro : CIP-005-1
3.	Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.	3.	Objet : La norme CIP-005 exige l'identification et la protection des périmètres de sécurité électroniques dans lesquels tous les actifs électroniques critiques résident ainsi que tous les points d'accès à ces périmètres.
	Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.		La norme CIP-005 fait partie d'un groupe de normes CIP-002 à CIP-009 et doit être lue dans ce contexte. Les entités responsables doivent interpréter et mettre en pratique les normes CIP-002 à CIP-009 tout en tenant raisonnablement compte des impératifs d'affaires qui s'imposent.
4.	Applicability:	4.	Applicabilité :
4.1	Within the text of Standard CIP-005, “Responsible Entity” shall mean:	4.1	Dans le contexte de la norme CIP-005, l'expression « entité responsable » désigne :
4.1.1	Reliability Coordinator	4.1.1	Coordonnateur de la fiabilité
4.1.2	Balancing Authority	4.1.2	Responsable de l'équilibrage
4.1.3	Interchange Authority	4.1.3	Responsable des échanges
4.1.4	Transmission Service Provider	4.1.4	Fournisseur de services de transport
4.1.5	Transmission Owner	4.1.5	Propriétaire du réseau de transport
4.1.6	Transmission Operator	4.1.6	Exploitant du réseau de transport
4.1.7	Generator Owner	4.1.7	Propriétaire d'installations de production
4.1.8	Generator Operator	4.1.8	Exploitant d'installations de production
4.1.9	Load Serving Entity	4.1.9	Responsable de l'approvisionnement
4.1.10	NERC	4.1.10	NERC
4.1.11	Regional Reliability Organizations	4.1.11	Organisations régionales de fiabilité

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
4.2	The following are exempt from Standard CIP-005:	4.2	Les entités suivantes sont exemptées de la norme CIP-005 :
4.2.1	Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.	4.2.1	Les installations réglementées par la <i>U.S. Nuclear Regulatory Commission</i> ou la Commission canadienne de sûreté nucléaire.
4.2.2	Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.	4.2.2	Les actifs électroniques associés aux réseaux de communication et aux liens de communication entre les périmètres de sécurité électroniques.
4.2.3	Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.	4.2.3	Les entités responsables qui, en conformité avec la norme CIP-002, ont prouvé qu'elles ne détiennent aucun actif électronique critique.
5.	Effective Date: June 1, 2006.	5.	Date d'entrée en vigueur : 1 ^{er} juin 2006

B. Requirements / Exigences

R1	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	E1	Périmètre de sécurité électronique — L'entité responsable doit s'assurer que chacun des actifs électroniques critiques se situe à l'intérieur d'un périmètre de sécurité électronique. L'entité responsable doit identifier et documenter le ou les périmètres de sécurité électroniques et tous les points d'accès à ces périmètres.
R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	E1.1	Les points d'accès aux périmètres de sécurité électroniques doivent inclure tout équipement de communication avec l'externe (p.ex., un modem commuté) dont l'extrémité est située à l'intérieur d'un périmètre de sécurité électronique.
R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	E1.2	Dans le cas d'un actif électronique critique à accès commuté utilisant un protocole non routable, l'entité responsable doit définir un périmètre de sécurité électronique pour ce point d'accès autour de l'équipement de communication commuté.
R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	E1.3	Les liens de communication qui relient des périmètres de sécurité électroniques ne doivent pas être considérés comme faisant partie du périmètre de sécurité électronique. Par contre, les extrémités de ces liens de communication qui se trouvent à l'intérieur des périmètres de sécurité électroniques doivent être considérées comme des points d'accès aux périmètres de sécurité électroniques.

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	E1.4	Tout actif électronique non critique se trouvant à l'intérieur d'un périmètre de sécurité électronique doit être identifié et protégé conformément aux exigences de la norme CIP-005.
R1.5	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	E1.5	Les actifs électroniques utilisés pour le contrôle ou la surveillance des accès aux périmètres de sécurité électroniques doivent se doter des mesures de protection décrites dans la norme CIP-003, l'exigence E3 de la norme CIP-004, les exigences E2 et E3 de la norme CIP-005, les exigences E2 et E3 de la norme CIP-006, les exigences E1 et E3 à E9 de la norme CIP-007, la norme CIP-008 et la norme CIP-009.
R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	E1.6	L'entité responsable doit gérer la documentation de ses périmètres de sécurité électroniques, de tous ses actifs interconnectés critiques et non critiques à l'intérieur de ces périmètres, de tous les points d'accès électroniques à ces périmètres et des actifs électroniques utilisés pour le contrôle et la surveillance de ces points d'accès.
R2	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	E2	Contrôle d'accès électronique — L'entité responsable doit mettre en place et documenter les processus organisationnels ainsi que les dispositifs techniques et les marches à suivre concernant le contrôle des accès électroniques à tous les points d'accès électroniques des périmètres de sécurité électroniques.
R2.1	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	E2.1	Ces processus et mécanismes doivent s'appuyer sur un modèle de contrôle qui, par défaut, refuse tout accès de telle sorte qu'il soit nécessaire de définir explicitement des permissions d'accès.
R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	E2.2	À tous les points d'accès des périmètres de sécurité électroniques, l'entité responsable doit activer seulement les ports et les services nécessaires pour l'exploitation et la surveillance des actifs électroniques à l'intérieur du périmètre de sécurité électronique, et doit documenter, de façon individuelle ou par groupe, la configuration de ces ports et de ces services.
R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	E2.3	L'entité responsable doit gérer une procédure permettant de sécuriser les accès commutés aux périmètres de sécurité électroniques.

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	E2.4	Aux endroits où l'accès interactif externe avec le périmètre de sécurité électronique est permis, l'entité responsable doit mettre en place des contrôles techniques ou procéduraux rigoureux aux points d'accès pour confirmer l'identité des personnes, là où la technologie le permet.
R2.5	The required documentation shall, at least, identify and describe:	E2.5	La documentation exigée doit au moins nommer et décrire :
R2.5.1	The processes for access request and authorization.	E2.5.1	Les processus de demande d'accès et d'autorisation
R2.5.2	The authentication methods.	E2.5.2	La méthode de confirmation d'identité
R2.5.3	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	E2.5.3	Le processus de révision des droits d'autorisation en vertu de l'exigence E4 de la norme CIP-004.
R2.5.4	The controls used to secure dial-up accessible connections.	E2.5.4	Les mécanismes de contrôle utilisés pour sécuriser les accès des connexions commutées.
R2.6	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	E2.6	Bandeau sur l'utilisation appropriée — Là où la technologie le permet, les dispositifs d'accès électronique doivent afficher un bandeau approprié à l'écran de l'utilisateur lors de toute tentative d'accès interactif. L'entité responsable doit conserver un document décrivant le contenu de la bannière.
R3	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	E3	Surveillance des accès électroniques — L'entité responsable doit mettre en place et documenter un ou des processus électroniques ou manuels pour la surveillance et la consignation des accès aux points d'accès des périmètres de sécurité électroniques, et ce, vingt-quatre heures sur vingt-quatre, sept jours sur sept.
R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	E3.1	Pour les accès commutés aux actifs électroniques critiques qui utilisent des protocoles non routables, l'entité responsable doit mettre en place et documenter les processus de surveillance à chaque point d'accès de l'équipement de communication commuté, là où la technologie le permet.

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	E3.2	Là où la technologie le permet, les processus de surveillance de la sécurité doivent détecter et émettre une alerte à la suite de toute tentative d'accès ou d'un accès non autorisé. Ces alertes doivent fournir des informations appropriées au personnel désigné. Aux endroits où les alertes ne sont techniquement pas possibles, l'entité responsable doit réviser ou vérifier les registres d'accès pour les tentatives d'accès ou les accès non autorisés, et ce, au moins à tous les 90 jours civils.
R4	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	E4	Analyse de la cybervulnérabilité — L'entité responsable doit effectuer une analyse de la cybervulnérabilité des points d'accès des périmètres de sécurité électroniques au moins une fois par année. L'analyse de la cybervulnérabilité doit inclure au moins un des points suivants :
R4.1	A document identifying the vulnerability assessment process;	E4.1	Un document décrivant les processus d'analyse de la cybervulnérabilité.
R4.2	A review to verify that only ports and services required for operations at these access points are enabled;	E4.2	Une vérification pour s'assurer que seuls les ports et les services nécessaires au fonctionnement de ces points d'accès sont activés.
R4.3	The discovery of all access points to the Electronic Security Perimeter;	E4.3	Le repérage de tous les points d'accès du périmètre de sécurité électronique.
R4.4	A review of controls for default accounts, passwords, and network management community strings; and,	E4.4	Une révision des mécanismes de contrôle des comptes par défaut, des mots de passe, des noms de communauté de gestion du réseau.
R4.5	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	E4.5	La documentation des résultats de l'analyse, le plan d'action visant à corriger ou à atténuer les vulnérabilités décelées dans le cadre de l'analyse, et l'état d'avancement du plan d'action.
R5	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	E5	Révision et mise à jour de la documentation — L'entité responsable doit réviser, mettre à jour et gérer toute la documentation nécessaire en vertu des exigences de la norme CIP-005.
R5.1	The Responsible Entity shall ensure that all documentation required by Standard CIP005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	E5.1	L'entité responsable doit s'assurer que toute la documentation exigée par la norme CIP-005 prend en compte les configurations et les processus actuels et doit réviser la documentation et les processus décrits dans la norme CIP-005 au moins une fois par année.

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
R5.2	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	E5.2	L'entité responsable doit mettre à jour la documentation pour qu'elle reflète la modification du réseau ou des mécanismes de contrôle dans les 90 jours civils suivant le changement.
R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	E5.3	L'entité responsable doit conserver les journaux des accès électroniques au moins pendant 90 jours ouvrables. Les journaux ayant trait à un incident déclaré doivent être conservés en vertu des exigences de la norme CIP-008.

C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-005 :
M1	Documents about the Electronic Security Perimeter as specified in Requirement R1.	M1	La documentation sur les périmètres de sécurité électroniques, conformément à l'exigence E1.
M2	Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.	M2	La documentation sur les mécanismes de contrôle d'accès aux périmètres de sécurité électroniques, conformément à l'exigence E2.
M3	Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.	M3	La documentation sur les mécanismes de contrôle mis en place pour la consignation et la surveillance des accès aux périmètres de sécurité électroniques, conformément à l'exigence E3.
M4	Documentation of the Responsible Entity's annual vulnerability assessment as specified in Requirement R4.	M4	La documentation sur l'analyse de la vulnérabilité annuelle de l'entité responsable, conformément à l'exigence E4.
M5	Access logs and documentation of review, changes, and log retention as specified in Requirement R5.	M5	Les journaux des accès et la documentation sur les révisions, les changements et la conservation des registres, conformément à l'exigence E5.

D. Compliance / Conformité

1.	Compliance Monitoring Process	1.	Processus de vérification de la conformité
1.1	Compliance Monitoring Responsibility	1.1	Responsabilité de la vérification de la conformité
1.1.1	Regional Reliability Organizations for Responsible Entities.	1.1.1	Les organisations régionales de fiabilité pour les entités responsables.
1.1.2	NERC for Regional Reliability Organization.	1.1.2	La NERC pour les organisations régionales de fiabilité.

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
1.1.3	Third-party monitor without vested interest in the outcome for NERC.	1.1.3	Un vérificateur tiers n'ayant pas d'intérêt quant aux résultats pour la NERC.
1.2	Compliance Monitoring Period and Reset Time Frame Annually.	1.2	Période de vérification de la conformité et délai de retour en conformité Annuelle
1.3	Data Retention	1.3	Conservation des données
1.3.1	The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.	1.3.1	L'entité responsable doit conserver les journaux d'exploitation pendant au moins 90 jours civils, à moins que la période de rétention soit plus longue, conformément à l'exigence E2 de la norme CIP-008.
1.3.2	The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.	1.3.2	L'entité responsable doit conserver toute la documentation et les dossiers de toute la dernière année civile, conformément à la norme CIP-005.
1.3.3	The compliance monitor shall keep audit records for three years.	1.3.3	Le vérificateur de la conformité doit garder les dossiers des audits des trois dernières années.
1.4	Additional Compliance Information	1.4	Autre information sur la conformité
1.4.1	Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.	1.4.1	L'entité responsable doit faire la preuve de sa conformité au moyen d'une autocertification ou d'une vérification, selon ce que déterminera le vérificateur de la conformité.
1.4.2	Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.	1.4.2	Les cas où l'entité responsable ne peut se conformer à sa politique de cybersécurité doivent être documentés et approuvés par le cadre supérieur désigné ou son (ses) délégué(s). Se reporter à la norme CIP-003, exigence E3. Les exceptions dûment autorisées ne conduiront pas à une non-conformité.
2.	Levels of Non-Compliance	2.	Niveaux de non-conformité
2.1	Level 1:	2.1	Niveau 1 :
2.1.1	All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,	2.1.1	Tous les documents requis en vertu de la norme CIP-005 existent, mais n'ont pas été mis à jour dans les 90 jours suivant tout changement tel qu'exigé; ou,
2.1.2	Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;	2.1.2	L'accès à moins de 15 % des périmètres de sécurité électroniques n'est pas contrôlé, surveillé et consigné dans un journal;

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
2.1.3	Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,	2.1.3	La documentation confirmant que seuls les ports et les services nécessaires ont été activés existe, mais il n'y a pas de dossier sur la révision annuelle; ou,
2.1.4	At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.	2.1.4	Au moins une, mais pas toutes, les analyses de vulnérabilité des périmètres de sécurité électroniques ont été effectuées durant la dernière année civile.
2.2	Level 2:	2.2	Niveau 2 :
2.2.1	All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,	2.2.1	Tous les documents requis par la norme CIP-005 existent, mais n'ont pas été mis à jour durant la dernière année civile tel qu'exigé; ou,
2.2.2	Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,	2.2.2	L'accès de 15 % à 25 % des périmètres de sécurité électroniques n'est pas contrôlé, surveillé et consigné dans un journal; ou,
2.2.3	Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.	2.2.3	La documentation et les dossiers sur les analyses de vulnérabilité des périmètres de sécurité existent, mais aucune analyse de vulnérabilité n'a été effectuée au cours de la dernière année civile.
2.3	Level 3:	2.3	Niveau 3 :
2.3.1	A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,	2.3.1	Un document qui définit les périmètres de sécurité électroniques existe, mais il y a au moins un actif électronique critique qui n'est pas dans un périmètre de sécurité électronique défini; ou,
2.3.2	One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,	2.3.2	Au moins un actif électronique non critique connu est dans un périmètre de sécurité électronique, mais ce n'est pas documenté; ou,
2.3.3	Electronic access controls document(s) exist, but one or more access points have not been identified; or,	2.3.3	La documentation sur les mécanismes de contrôle d'accès existe, mais au moins un point d'accès n'a pas été identifié; ou,
2.3.4	Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,	2.3.4	La documentation sur les mécanismes de contrôle d'accès n'identifie pas ou ne décrit pas les mécanismes de contrôle d'au moins un point d'accès; ou,
2.3.5	Electronic Access Monitoring:	2.3.5	Surveillance des accès électroniques :
2.3.5.1	Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,	2.3.5.1	L'accès de 26 % à 50 % des périmètres de sécurité électroniques n'est pas contrôlé, surveillé et consigné dans un journal; ou,

Traduction française de la norme de la NERC CIP-005-1

Cyber Security — Electronic Security Perimeter(s)

Cybersécurité — Périmètres de sécurité électroniques

Ch.	English Version		Version française
2.3.5.2	Access logs exist, but have not been reviewed within the past ninety calendar days; or,	2.3.5.2	Les journaux des accès existent, mais n'ont pas été vérifiés au cours des 90 derniers jours civils; ou,
2.3.6	Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.	2.3.6	La documentation et les dossiers d'analyse de vulnérabilité des périmètres de sécurité électroniques existent, mais aucune analyse de vulnérabilité n'a été effectuée depuis plus de deux années civiles.
2.4	Level 4:	2.4	Niveau 4 :
2.4.1	No documented Electronic Security Perimeter exists; or,	2.4.1	Aucune documentation sur les périmètres de sécurité électroniques n'existe; ou,
2.4.2	No records of access exist; or,	2.4.2	Aucun dossier sur les accès n'existe; ou,
2.4.3	51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,	2.4.3	L'accès à 51 % et plus des périmètres de sécurité électroniques n'est pas contrôlé, surveillé et consigné dans un journal; ou,
2.4.4	Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,	2.4.4	La documentation et les dossiers d'analyse de vulnérabilité des périmètres de sécurité électroniques existent, mais aucune analyse de vulnérabilité n'a été effectuée depuis plus de trois années civiles; ou,
2.4.5	No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.	2.4.5	La documentation sur l'analyse de vulnérabilité des périmètres de sécurité électroniques n'existe pas.

E. Regional Differences / Différences régionales

1.	None identified.	1.	Aucune n'a été établie.
----	------------------	----	-------------------------

Version History

Version	Date	Action	Change Tracking
1		D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended	03/24/06

Historique des versions

Version	Date	Intervention	Suivi des modifications
1	16 janvier 2006	D.2.3.1 — Remplacer « Critical Assets » par « Critical Cyber Assets », tel que prévu, dans la version anglaise	24 mars 2006