

**TABLE OF CONTENTS**

**TABLE DES MATIÈRES**

**A. INTRODUCTION**

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

**B. REQUIREMENTS**

R1 to R6

**C. MEASURES**

M1 to M6

**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 E6

**C. MESURES**

M1 à M6

**D. CONFORMITÉ**

- 1. Processus de vérification de la conformité
  - 1.1 Responsabilité de 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-006-1

*Cyber Security — Physical Security of Critical Cyber Assets*

*Cybersécurité — Sécurité physique des actifs électroniques critiques*

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

## A. Introduction / Introduction

1.	<b>Title:</b> Cyber Security — Physical Security of Critical Cyber Assets	1.	<b>Titre :</b> Cybersécurité — Sécurité physique des actifs électroniques critiques
2.	<b>Number:</b> CIP-006-1	2.	<b>Numéro :</b> CIP-006-1
3.	<b>Purpose:</b> Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.	3.	<b>Objet :</b> La norme CIP-006 a pour but d'assurer la mise en place d'un programme de sécurité physique pour la protection des actifs électroniques critiques.
	Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.		La norme CIP-006 fait partie d'un groupe de normes CIP-002 à CIP-009 et doit être lue dans ce contexte. Les entités responsables doivent mettre en pratique les normes CIP-002 à CIP-009 tout en tenant raisonnablement compte des impératifs d'affaires.
4.	<b>Applicability:</b>	4.	<b>Applicabilité :</b>
4.1	Within the text of Standard CIP-006, “Responsible Entity” shall mean :	4.1	Dans le contexte de la norme CIP-006, 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
4.2	The following are exempt from Standard CIP-006:	4.2	Les entités suivantes sont exemptées de la norme CIP-006 :

## Traduction française de la norme de la NERC CIP-006-1

### Cyber Security — Physical Security of Critical Cyber Assets

### Cybersécurité — Sécurité physique des actifs électroniques critiques

Ch.	English Version		Version française
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 électronique.
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.	<b>Effective Date:</b> June 1, 2006.	5.	<b>Date d'entrée en vigueur :</b> 1 <sup>er</sup> juin 2006.

## B. Requirements / Exigences

R1	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	E1	Plan de sécurité physique — L'entité responsable doit créer et gérer un plan de sécurité physique, approuvé par un cadre supérieur ou un ou des délégués, qui doit porter minimalement sur les points suivants :
R1.1	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.	E1.1	Les processus requis pour s'assurer que tous les actifs électroniques à l'intérieur du périmètre de sécurité électronique résident également à l'intérieur d'un périmètre de sécurité physique et le documenter. Lorsqu'un périmètre physique complètement étanche (« six parois ») ne peut être établi, l'entité responsable doit déployer et documenter des mesures de rechange pour contrôler l'accès physique aux actifs électroniques critiques.
R1.2	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	E1.2	Les processus d'identification de tous les points d'accès de chaque périmètre de sécurité physique et les mesures de contrôle des entrées pour ces points d'accès.
R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	E1.3	Les processus, les outils, et les procédures de surveillance des accès physiques aux périmètres.
R1.4	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	E1.4	Les procédures pour l'utilisation appropriée des mécanismes de contrôle d'accès physiques tel que décrit dans l'exigence E3 incluant la gestion des cartes d'accès des visiteurs, les actions en cas de perte et l'interdiction d'une mauvaise utilisation des mécanismes de contrôle d'accès physique.
R1.5	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	E1.5	Procédures pour la révision des demandes d'autorisation d'accès et la révocation des autorisations d'accès, selon l'exigence E4 de la norme CIP-004.

## Traduction française de la norme de la NERC CIP-006-1

### *Cyber Security — Physical Security of Critical Cyber Assets*

### *Cybersécurité — Sécurité physique des actifs électroniques critiques*

Ch.	English Version		Version française
R1.6	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	E1.6	Les procédures relatives à l'accès accompagné à l'intérieur d'un périmètre de sécurité physique du personnel qui ne dispose pas d'accès sans escorte.
R1.7	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	E1.7	Les processus de mise à jour du plan de sécurité physique dans les 90 jours suivant un changement d'aménagement ou de configuration d'un système de sécurité physique, incluant, mais sans s'y limiter, l'ajout ou le retrait d'un point d'accès au périmètre de sécurité physique, les mécanismes de contrôle d'accès physique, le système de surveillance ou les systèmes de consignment.
R1.8	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement E2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	E1.8	Les actifs électroniques utilisés pour le contrôle et la surveillance du périmètre de sécurité physique doivent utiliser les mesures de protection spécifiées 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, la norme CIP-007, la norme CIP-008 et la norme CIP-009.
R1.9	Process for ensuring that the physical security plan is reviewed at least annually.	E1.9	Le processus pour s'assurer que le plan de sécurité physique est révisé au moins une fois par année.
R2	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:	E2	Mécanismes de contrôle de l'accès physique — L'entité responsable doit documenter et mettre en place les processus de fonctionnement et les procédures de contrôle pour la gestion de tous les points d'accès physiques des périmètres de sécurité physiques, et ce, vingt-quatre heures sur vingt-quatre, sept jours sur sept. L'entité responsable doit mettre en place une ou plusieurs des méthodes d'accès physique suivantes :
R2.1	Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.	E2.1	Carte d'accès : Un dispositif d'accès électronique pour lequel les droits d'accès du détenteur sont prédéfinis dans une base de données. Les droits d'accès peuvent être différents d'un périmètre à un autre.
R2.2	Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.	E2.2	Systèmes de verrouillage : Celles-ci incluent, mais sans s'y limiter, les serrures à « clé à copie restreinte », les serrures magnétiques qui peuvent être déverrouillées à distance et les sas de sécurité.
R2.3	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	E2.3	Personnel de sécurité : Personne responsable de la surveillance des accès physiques, qui peut être sur place ou dans une station de surveillance à distance.

## Traduction française de la norme de la NERC CIP-006-1

### *Cyber Security — Physical Security of Critical Cyber Assets*

### *Cybersécurité — Sécurité physique des actifs électroniques critiques*

Ch.	English Version		Version française
R2.4	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	E2.4	Autres dispositifs d'authentification : biométrie, serrure à clavier numérique, jeton ou tout autre dispositif permettant de surveiller l'accès physique aux actifs électroniques critiques.
R3	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:	E3	Surveillance des accès physiques — L'entité responsable doit documenter et mettre en place la technologie et les procédures de contrôle pour la surveillance des accès physiques de tous aux points d'accès aux périmètres de sécurité électroniques, et ce, vingt-quatre heures sur vingt-quatre, sept jours sur sept. Les tentatives d'accès non autorisées doivent faire l'objet d'un suivi immédiat et être traitées conformément à la norme CIP-008. Une ou plusieurs des méthodes de surveillance suivantes doivent être utilisées :
R3.1	Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.	E3.1	Système d'alarme : Le système doit émettre une alarme pour indiquer qu'une porte, une barrière ou une fenêtre a été ouverte sans autorisation. L'alarme doit être transmise immédiatement au personnel responsable des interventions.
R3.2	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	E3.2	Surveillance humaine aux points d'accès : La surveillance des points d'accès doit se faire par une personne autorisée, conformément à l'exigence E2.3.
R4	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:	E4	Consignation des accès physiques — La consignation des données d'accès doit contenir l'information nécessaire à l'identification de chaque personne au moment de l'accès, et ce, vingt-quatre heures sur vingt-quatre, sept jours sur sept. L'entité responsable doit mettre en place et documenter les mécanismes techniques et la procédure de consignation des accès physiques de tous les points d'accès des périmètres de sécurité physiques en utilisant l'une ou plusieurs des méthodes de consignation suivante ou leur équivalent :
R4.1	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	E4.1	Consignation informatique : Journaux électroniques produits selon la méthode de surveillance adoptée par l'entité responsable.
R4.2	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	E4.2	Enregistrement vidéo : Saisie électronique d'image vidéo de qualité suffisante pour permettre l'identification d'une personne.

## Traduction française de la norme de la NERC CIP-006-1

### Cyber Security — Physical Security of Critical Cyber Assets

### Cybersécurité — Sécurité physique des actifs électroniques critiques

Ch.	English Version		Version française
R4.3	Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.	E4.3	Consignation manuelle : Un journal, une feuille de signature, ou un autre rapport de consignation des accès physiques remplis par un gardien de sécurité ou une autre personne autorisée à surveiller les accès physiques conformément à l'exigence E2.3.
R5	Access Log Retention — The responsible entity shall retain physical 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	Conservation des journaux des accès — L'entité responsable doit conserver les journaux des accès physiques pendant au moins 90 jours civils. Les journaux ayant trait à un incident déclaré doivent être conservés conformément aux exigences de la norme CIP-008.
R6	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	E6	Maintenance et essais — L'entité responsable doit mettre en place un programme de maintenance et d'essais pour s'assurer que tous les systèmes de sécurité physique tels que décrits dans les exigences E2, E3, et E4 fonctionnent correctement. Le programme doit inclure au moins les tâches suivantes :
R6.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	E6.1	La maintenance et les essais de tous les mécanismes de sécurité physique au cours d'un cycle maximal de 3 ans.
R6.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	E6.2	La conservation des données de maintenance et d'essais au cours d'un cycle déterminé par l'entité responsable conformément à l'exigence E6.1.
R6.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	E6.3	La conservation des données d'interruption relatives aux mécanismes de contrôle des accès, aux transactions d'accès, et la surveillance pour un minimum d'une année.

### C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:		Les mesures suivantes seront utilisées pour valider la conformité aux exigences de la norme CIP-006 :
M1	The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.	M1	Le plan de sécurité physique conformément à l'exigence E1 et la documentation sur la révision et la mise à jour du plan.
M2	Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.	M2	La documentation décrivant les méthodes de contrôle des accès physiques à chaque point d'accès d'un périmètre de sécurité physique conformément à l'exigence E2.
M3	Documentation identifying the methods for monitoring physical access as specified in Requirement R3.	M3	La documentation décrivant les méthodes de surveillance des accès physiques conformément à l'exigence E3.

## Traduction française de la norme de la NERC CIP-006-1

*Cyber Security — Physical Security of Critical Cyber Assets*

*Cybersécurité — Sécurité physique des actifs électroniques critiques*

Ch.	English Version		Version française
M4	Documentation identifying the methods for logging physical access as specified in Requirement R4.	M4	La documentation décrivant les méthodes de consignation des données relatives aux accès physiques conformément à l'exigence E4.
M5	Access logs as specified in Requirement R5.	M5	Les journaux des accès, conformément à l'exigence E5.
M6	Documentation as specified in Requirement R6.	M6	La documentation conformément à l'exigence E6.

### D. Compliance / Conformité

1.	<b>Compliance Monitoring Process</b>	1.	<b>Processus de vérification de la conformité</b>
1.1	<b>Compliance Monitoring Responsibility</b>	1.1	<b>Responsabilité de la vérification de la conformité</b>
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.
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	<b>Compliance Monitoring Period and Reset Time Frame</b> Annually.	1.2	<b>Période de vérification de la conformité et délai de retour en conformité</b> Annuelle
1.3	<b>Data Retention</b>	1.3	<b>Conservation des données</b>
1.3.1	The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.	1.3.1	L'entité responsable doit conserver toute la documentation de la dernière année civile sauf celle décrite dans les exigences E5 et E6.2.
1.3.2	The compliance monitor shall keep audit records for three calendar years.	1.3.2	Le vérificateur de la conformité doit garder les dossiers d'audit durant trois années civiles.
1.4	<b>Additional Compliance Information</b>	1.4	<b>Autre information sur la conformité</b>
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 démontrer son respect des exigences par un processus d'autocertification ou un audit, tel que déterminé par le vérificateur de la conformité.

## Traduction française de la norme de la NERC CIP-006-1

### *Cyber Security — Physical Security of Critical Cyber Assets*

### *Cybersécurité — Sécurité physique des actifs électroniques critiques*

Ch.	English Version		Version française
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 d'exception 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 ou ses délégués. Se reporter à l'exigence E3 de la norme CIP-003. Les exceptions dûment autorisées ne conduiront pas à une non-conformité.
1.4.3	The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.	1.4.3	L'entité responsable ne devrait pas faire d'exception dans sa politique de cybersécurité pour la création, la documentation ou la maintenance d'un plan de sécurité physique.
1.4.4	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.	1.4.4	Dans le cas d'un actif électronique critique à accès commuté utilisant un protocole non routable, l'entité responsable n'est pas tenue de se conformer à la norme CIP-006 en ce qui a trait à ce point d'accès autour de l'équipement de communication commuté.
2.	<b>Levels of Non-Compliance</b>	2.	<b>Niveaux de non-conformité</b>
2.1	<b>Level 1:</b>	2.1	<b>Niveau 1 :</b>
2.1.1	The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,	2.1.1	Le plan de sécurité physique existe, mais n'a pas été mis à jour dans les 90 jours civils suivant une modification du plan ou de n'importe laquelle de ses composantes; ou,
2.1.2	Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,	2.1.2	L'accès à moins de 15 % du total des périmètres de sécurité physiques d'une entité responsable n'est pas contrôlé, surveillé et consigné dans un journal; ou,
2.1.3	Required documentation exists but has not been updated within ninety calendar days of a modification.; or,	2.1.3	La documentation exigée existe, mais n'a pas été mise à jour dans les 90 jours suivant une modification; ou,
2.1.4	Physical access logs are retained for a period shorter than ninety days; or,	2.1.4	Les journaux des accès physiques sont conservés pour une période plus courte que 90 jours; ou,
2.1.5	A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,	2.1.5	Un programme de maintenance et d'essais pour les systèmes de sécurité physiques existe, mais tous les systèmes n'ont pas été testés à l'intérieur des cycles exigés; ou,
2.1.6	One required document does not exist.	2.1.6	Un document exigé n'existe pas.
2.2	<b>Level 2:</b>	2.2	<b>Niveau 2 :</b>
2.2.1	The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,	2.2.1	Le plan de sécurité physique existe, mais n'a pas été mis à jour dans les six mois suivant une modification du plan ou n'importe laquelle de ses composantes; ou,

## Traduction française de la norme de la NERC CIP-006-1

### *Cyber Security — Physical Security of Critical Cyber Assets*

### *Cybersécurité — Sécurité physique des actifs électroniques critiques*

Ch.	English Version		Version française
2.2.2	Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,	2.2.2	L'accès à une proportion de 15 % à 25 % du nombre total des périmètres de sécurité physiques de l'entité responsable n'est pas contrôlé, surveillé et consigné dans un journal; ou
2.2.3	Required documentation exists but has not been updated within six calendar months of a modification; or	2.2.3	La documentation exigée existe, mais n'a pas été mise à jour dans les six mois civils suivant une modification; ou,
2.2.4	More than one required document does not exist.	2.2.4	Plus d'un document exigé n'existe pas.
2.3	<b>Level 3:</b>	2.3	<b>Niveau 3 :</b>
2.3.1	The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,	2.3.1	Le plan de sécurité physique existe, mais n'a pas été mis à jour dans les douze mois civils suivant une modification du plan ou n'importe laquelle de ses composantes; ou,
2.3.2	Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,	2.3.2	L'accès à une proportion de 26 % à 50 % du nombre total des accès aux périmètres de sécurité physiques de l'entité responsable n'est pas contrôlé, surveillé et consigné dans un journal ou,
2.3.3	No logs of monitored physical access are retained.	2.3.3	Aucun journal des accès physiques surveillés n'est conservé.
2.4	<b>Level 4:</b>	2.4	<b>Niveau 4 :</b>
2.4.1	No physical security plan exists; or,	2.4.1	Aucun plan de sécurité physique n'existe; ou,
2.4.2	Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,	2.4.2	L'accès à une proportion de plus de 51 % du nombre total des périmètres de sécurité physiques de l'entité responsable n'est pas contrôlé, surveillé et consigné dans un journal; ou,
2.4.3	No maintenance or testing program exists.	2.4.3	Aucun programme de maintenance et d'essais n'existe.

### **E. Regional Differences / Différences régionales**

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

## Traduction française de la norme de la NERC CIP-006-1

*Cyber Security — Physical Security of Critical Cyber Assets*

*Cybersécurité — Sécurité physique des actifs électroniques critiques*

### Version History

Version	Date	Action	Change Tracking
1	06/01/06	Effective Date	New

### Historique des versions

Version	Date	Intervention	Suivi des modifications
1	1 <sup>er</sup> juin 2006	Date d'entrée en vigueur	Nouvelle norme