

**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 E4

**C. MESURES**

M1 à M4

**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**

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

**A. Introduction / Introduction**

1.	<b>Title:</b> Cyber Security — Critical Cyber Asset Identification.	1.	<b>Titre :</b> Cybersécurité — Identification des actifs électroniques critiques
2.	<b>Number:</b> CIP-002-1	2.	<b>Numéro :</b> CIP-002-1
3.	<b>Purpose:</b> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.	3.	<b>Objet :</b> Les normes de la NERC CIP-002 à CIP-009 établissent un cadre de cybersécurité permettant l'identification et la protection des actifs électroniques critiques dans le but de soutenir l'exploitation fiable du réseau de transport principal.
	These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.		Ces normes font état du rôle distinct de chaque entité en ce qui a trait à l'exploitation du réseau de transport principal, à la criticité et à la vulnérabilité des actifs nécessaires à la gestion de la fiabilité du réseau de transport principal, et aux risques auxquels ils sont exposés. 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.
	Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.		Les contraintes d'exploitation et d'affaires dans la gestion et le maintien de la fiabilité du réseau de transport principal reposent de plus en plus sur les actifs électroniques qui prennent en charge des fonctions et des processus critiques liées à la fiabilité tout en assurant la communication de données et de services entre eux, entre les fonctions et entre les organisations. Cela entraîne des risques accrus pour ces actifs électroniques.
	Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.		La norme CIP-002 exige l'identification et la documentation des actifs électroniques critiques associés aux actifs critiques qui prennent en charge l'exploitation fiable du réseau de transport principal. Ces actifs critiques doivent être identifiés grâce à une analyse des risques.
4.	<b>Applicability:</b>	4.	<b>Applicabilité :</b>
4.1	Within the text of Standard CIP-002, "Responsible Entity" shall mean :	4.1	Dans le contexte de la norme CIP-002, 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

## Traduction française de la norme de la NERC CIP-002-1

### Cyber Security — Critical Cyber Asset Identification

### Cybersécurité — Identification des actifs électroniques critiques

Ch.	English Version		Version française
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-002 :	4.2	Les entités suivantes sont exemptées de la norme CIP-002 :
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 discrets.
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	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	E1	Méthode d'identification des actifs critiques — L'entité responsable doit identifier et documenter la méthode d'analyse des risques utilisée pour identifier ses actifs critiques.
R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	E1.1	L'entité responsable doit maintenir la documentation décrivant sa méthode d'analyse des risques qui comprend les procédures et les critères d'évaluation.
R1.2	The risk-based assessment shall consider the following assets:	E1.2	L'analyse des risques doit porter sur les actifs suivants :

## Traduction française de la norme de la NERC CIP-002-1

### Cyber Security — Critical Cyber Asset Identification

### Cybersécurité — Identification des actifs électroniques critiques

Ch.	English Version		Version française
R1.2.1	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	E1.2.1	Les centres de contrôle et les centres de repli qui réalisent les activités des entités citées à la rubrique Applicabilité de la présente norme.
R1.2.2	Transmission substations that support the reliable operation of the Bulk Electric System.	E1.2.2	Les postes de transport qui assurent l'exploitation fiable du réseau de transport principal.
R1.2.3	Generation resources that support the reliable operation of the Bulk Electric System.	E1.2.3	Les ressources de production qui assurent l'exploitation fiable du réseau de transport principal.
R1.2.4	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	E1.2.4	Les systèmes et les installations critiques à la remise en charge du réseau, incluant les unités de production et les postes à démarrage autonome situés sur le trajet électrique des lignes de transport utilisées pour la remise en charge initiale du réseau.
R1.2.5	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	E1.2.5	Les systèmes et les installations critiques qui servent au délestage de charges, et qui d'un seul point de commande, peuvent délester 300 MW ou plus.
R1.2.6	Special Protection Systems that support the reliable operation of the Bulk Electric System.	E1.2.6	Les automatismes de réseau qui assurent l'exploitation fiable du réseau de transport principal.
R1.2.7	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	E1.2.7	Tout actif supplémentaire qui assure l'exploitation fiable du réseau de transport principal et que l'entité responsable juge approprié d'inclure dans son analyse.
R2	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	E2	Identification des actifs critiques — L'entité responsable doit dresser la liste de ses actifs critiques définis par la mise en application annuelle de sa méthode d'analyse des risques requise en vertu de l'exigence E1. L'entité responsable doit revoir cette liste au moins une fois par année et la mettre à jour au besoin.

Ch.	English Version		Version française
R3	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	E3	Identification d'actifs électroniques critiques — À l'aide de la liste des actifs critiques établie en vertu de l'exigence E2, l'entité responsable doit dresser une liste des actifs électroniques critiques au fonctionnement des actifs critiques. Par exemple, aux centres de contrôle et aux centres de repli, on trouve les systèmes et les installations liés aux sites principaux et aux centres à distance qui assurent la surveillance et le contrôle, le réglage automatique de la production, la modélisation du réseau en temps réel, et les échanges de données en temps réel entre les entreprises de service public d'électricité. L'entité responsable doit revoir cette liste au moins une fois par année et la mettre à jour au besoin. Aux fins de la norme CIP-002, les actifs électroniques critiques sont également définis comme étant ceux qui ont au moins l'une des caractéristiques suivantes :
R3.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	E3.1	L'actif électronique utilise un protocole « routable » pour communiquer à l'extérieur du périmètre électronique de sécurité; ou,
R3.2	The Cyber Asset uses a routable protocol within a control center; or,	E3.2	L'actif électronique utilise un protocole « routable » à l'intérieur du centre de contrôle; ou,
R3.3	The Cyber Asset is dial-up accessible.	E3.3	L'actif électronique est accessible par ligne commutée.
R4	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null).	E4	Approbation annuelle — Un cadre supérieur ou son (ses) délégué(s) doit (doivent) approuver annuellement la liste des actifs critiques et la liste des actifs électroniques critiques. En vertu des exigences E1, E2, et E3, l'entité responsable peut déterminer qu'elle n'a pas d'actifs critiques ou d'actifs électroniques critiques. L'entité responsable doit conserver un enregistrement daté et signé de l'approbation du cadre supérieur ou de son (ses) délégué(s) de la liste des actifs critiques et de la liste des actifs électroniques critiques (même si ces listes sont vides).

### C. Measures / Mesures

	The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:		Les mesures suivantes serviront à établir la preuve de la conformité aux exigences de la norme CIP-002 :
M1	The risk-based assessment methodology documentation as specified in Requirement R1.	M1	La documentation sur la méthode d'analyse des risques conformément à l'exigence E1.
M2	The list of Critical Assets as specified in Requirement R2.	M2	La liste des actifs critiques conformément à l'exigence E2.

Ch.	English Version		Version française
M3	The list of Critical Cyber Assets as specified in Requirement R3.	M3	La liste des actifs électroniques critiques conformément à l'exigence E3.
M4	The records of annual approvals as specified in Requirement R4.	M4	L'enregistrement des approbations annuelles conformément à l'exigence E4.

#### 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 documentation required by Standard CIP-002 from the previous full calendar year.	1.3.1	L'entité responsable doit conserver toute la documentation requise en vertu de la norme CIP-002 pour la dernière année civile.
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 des audits des trois dernières 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 faire la preuve de sa conformité au moyen d'une autocertification ou d'une vérification, selon ce que déterminera le vérificateur de la conformité.
2.	<b>Levels of Non-Compliance</b>	2.	<b>Niveaux de non-conformité</b>
2.1	<b>Level 1:</b> The risk assessment has not been performed annually.	2.1	<b>Niveau 1 :</b> L'analyse des risques n'a pas été faite annuellement.
2.2	<b>Level 2:</b> The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.	2.2	<b>Niveau 2 :</b> La liste des actifs critiques ou des actifs critiques électroniques existe, mais elle n'a pas été approuvée ou passée en revue au cours de la dernière année.

Ch.	English Version		Version française
2.3	<b>Level 3:</b> The list of Critical Assets or Critical Cyber Assets does not exist.	2.3	<b>Niveau 3 :</b> La liste des actifs critiques ou des actifs critiques électroniques n'existe pas.
2.4	<b>Level 4:</b> The lists of Critical Assets and Critical Cyber Assets do not exist.	2.4	<b>Niveau 4 :</b> Les listes des actifs critiques et des actifs critiques électroniques n'existent pas.

#### E. Regional Differences / Différences régionales

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

#### Version History

Version	Date	Action	Change Tracking
0	01/16/06	Effective Date	New
1	03/24/06	R3.2 — Change “Control Center” to “control center”	

#### Historique des versions

Version	Date	Intervention	Suivi des modifications
0	16 janvier 2006	Date d'entrée en vigueur	Nouvelle norme
1	24 mars 2006	E3.2 — Remplacer « Control Center » par « control center » dans la version anglaise	