
Project QC-2014-02**Standards CIP-002-5 through CIP-009-5 and standards CIP-010-1 and CIP-011-1****Critical Infrastructure Protection**

1. ASSESSMENT OF RELEVANCE

Over the past two decades, the operating tools of the interconnected power systems have evolved significantly. Deployment of computerized components, inter-connected smart devices and next-generation telecommunications networks has considerably improved the reliability of the electricity service. The integration of these new technologies has also introduced new risks related to cyber threats and the potential damage that they can cause.

Protecting the electricity grid from cyber attacks is a critical national security issue. Recent evidence suggests that cyber attacks on key energy infrastructure—and on the electricity system in particular—are increasing, both in frequency and sophistication. These trends are alarming because the potential consequences of a successful large-scale cyber attack on the electric power sector are difficult to overstate. As previous major grid failures, have shown, any event that causes prolonged power outages over a large area would not only be extremely costly, it would also severely impact millions of people's daily lives and could profoundly disrupt the delivery of essential services, including communications, food, water, health care, and emergency response. Moreover, cyber threats, unlike traditional threats to electric grid reliability such as extreme weather, are less predictable in their timing and more difficult to anticipate and address. In effect, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which is part of the U.S. Department of Homeland Security (DHS), reported responding to 198 cyber incidents in fiscal year 2012 across all critical infrastructure sectors. Forty-one percent of these incidents involved the energy sector, particularly electricity. The risk of a successful attack is significant.

The continued adoption and evolution of cyber security standards is thus required to protect the interconnected power system against the threats mentioned above. Version 5 of the CIP standards (CIP-002-5 through CIP-009-5 as well as standards CIP-010-1 and CIP-011-1) represent a significant improvement over the CIP version 1 standards adopted by the Régie under the R-3699-2009 filing. This new version is strengthened by four years of acquired experience by the North American electricity industry in the application of versions 1 and 3 of these standards.¹ Although the framework for implementation of the new CIP standards as a whole remains similar, the CIP-002-5 standard proposes a new process for identifying critical assets of the bulk electric system by identifying and categorizing the electronic systems associated with these assets. The standards CIP-003-5 through CIP-011-1 will therefore apply to the electronic systems identified under the CIP-002-5 standard. Among the notable enhancements, we find:

- The usage of clear and defined bright-line classification criteria to identify elements critical to the operation of the transmission system, making for a more uniform and objective identification.

¹ The CIP standards versions 2 and 4 never entered into force.

- The usage of an approach based on the National Institute of Standards and Technology (NIST) for categorizing systems impact on the bulk electric system (Impacts "Low", "Medium", or "High"). This approach allows to adequately secure systems according to their actual impact.
- The elimination of unnecessary documentation requirements to allow entities to focus on the reliability and the security of the transport network.
- Background and guiding principles included in each standard for implementation by the entities.
- The treatment of all modification directives issued by FERC Order 706.

The proposed CIP standards satisfy the reliability objective of defining a complete and consistent cybersecurity framework for the identification and protection of electronic systems that are necessary for the reliable operation of the interconnected transmission networks. The CIP standards can be separated into two categories:

- 1) Categorization of risk (Low, Medium or High)
 - CIP-002-5.1 – Cyber Security - BES Cyber System Categorization
- 2) Risk mitigation life cycle (implementation, assessment, monitoring and updates)
 - CIP-003-5 – Cyber Security -Security Management Controls
 - CIP-004-5.1 – Cyber Security -Personnel & Training
 - CIP-005-5 – Cyber Security - Electronic Security Perimeter(s)
 - CIP-006-5 – Cyber Security -Physical Security of BES Cyber Systems
 - CIP-007-5 – Cyber Security -System Security Management
 - CIP-008-5 – Cyber Security -Incident Reporting and Response Planning
 - CIP-009-5 – Cyber Security -Recovery Plans for BES Cyber Systems
 - CIP-010-1 – Cyber Security - Configuration Change Management and Vulnerability Assessments
 - CIP-011-1 – Cyber Security -Information Protection

The CIP-002-5 standard, which consists of the identification and classification of systems, is the first step of the cybersecurity network. An entity that has not identified any systems in compliance with the CIP-002-5 standard will not have to comply with the standards CIP-003-5 through CIP-011-1.

2. PREREQUISITE FOR ADOPTION

Adoption of the proposed definitions in the next section.

3. MODIFICATIONS TO OTHER STANDARDS OR TO GLOSSARY DEFINITIONS

The following additions, modifications or withdrawals have the same effective dates as the proposed standards.

3.1. Standards or requirements to be removed upon enforcement:

Standards CIP-002-1 through CIP-009-1.

3.2. New definitions to be added to the glossary:

Terme	Acronym	Definition
BES Cyber Asset		<p>A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)</p> <p>(Actif électronique BES)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
BES Cyber System		<p>One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.</p> <p>(Système électronique BES)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>

Terme	Acronym	Definition
BES Cyber System Information		<p>Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.</p> <p>(Information de système électronique BES)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>
CIP Exceptional Circumstance		<p>A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.</p> <p>(Circonstance CIP exceptionnelle)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>
CIP Senior Manager		<p>A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.</p> <p>(Cadre supérieur CIP)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>

Terme	Acronym	Definition
Control Center		<p>One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.</p> <p>(Centre de contrôle)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Dial-up Connectivity		<p>A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.</p> <p>(Connectivité par lien commuté)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Electronic Access Control or Monitoring Systems	EACMS	<p>Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.</p> <p>(Systèmes de contrôle ou de surveillance des accès électroniques)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Electronic Access Point	EAP	<p>A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.</p> <p>(Point d'accès électronique)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
External Routable Connectivity		<p>The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.</p> <p>(Connectivité externe routable)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>

Terme	Acronym	Definition
Interactive Remote Access		<p>User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.</p> <p>(Accès distant interactif)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Intermediate System		<p>A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.</p> <p>(Système intermédiaire)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Physical Access Control Systems	PACS	<p>Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.</p> <p>(Systèmes de contrôle des accès physiques)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Protected Cyber Assets	PCA	<p>One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes</p> <p>(Actifs électroniques protégés)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>

Terme	Acronym	Definition
Reportable Cyber Security Incident		<p>A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.</p> <p>(Incident de cybersécurité à déclarer)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>

3.3. Definitions to be modified in the glossary:

Terme	Acronym	Definition
Cyber Assets		<p>Programmable electronic devices, and communication networks including the hardware, software, and data <u>in those devices</u></p> <p>(Actifs électroniques)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Cyber Security Incident		<p>Any A malicious act or suspicious event that:</p> <ul style="list-style-type: none"> Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset BES Cyber System. <p>(Incident de cybersécurité)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Electronic Security Parameter	ESP	<p>The logical border surrounding a network to which Critical Cyber Assets <u>BES Cyber Systems</u> are connected using a <u>routable protocol</u> and for which access is controlled.</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>
Physical Security Perimeter	PSP	<p>The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.</p> <p>The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.</p> <p>(Périmètre de sécurité physique)</p> <p>Source: Glossary of Terms Used in NERC Reliability Standards</p>

3.4. Definitions to be removed from the glossary:

Terme	Acronym	Definition
Critical Assets		Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System (Actifs critiques) <small>Source: Glossary of Terms Used in NERC Reliability Standards</small>
Critical Cyber Assets		Cyber Assets essential to the reliable operation of Critical Assets. (Actifs électroniques critiques) <small>Source: Glossary of Terms Used in NERC Reliability Standards</small>

4. MODIFICATIONS TO THE REGISTER OF ENTITIES

In the format now under consideration by the Régie de l'énergie, the registry identifies assets that are critical as defined in version 1 of the CIP standards. The assessment required by the CIP-002-1 standard was completed by the Coordinator for all of Québec. With the new application framework of the CIP standards requiring identification of electronic systems, the Coordinator will no longer perform this analysis for the registered entities. Moreover, the list of elements considered critical is specific to activities for each entity and should be continuously monitored and reviewed. This information can therefore not be recorded in the register. Applicable entities, under the CIP-002-5 standard, will have to complete their own analysis of their assets and systems to determine if the standard applies to them. Consequently, the register will be modified to remove any information with regard to critical assets. Firstly, the "Assets classified as critical for CIP standards" information will be removed. Secondly, the "critical assets" column from the appendices for the transportation facilities, production facilities, telecommunication centers and operating centers will also be removed.

Note that since the register is currently under consideration by the Régie under the filing R-3699-2009, these changes will be made and filed with the Régie once a final decision has been rendered in the filing.

5. NOTE REGARDING THE USE OF THE TERM "POSTE" IN THE FRENCH VERSION

The English version of the standards uses the term "stations" and "substations" to designate a set of transmission elements in the same location. The term "substation" is often used in the industry to specify a station that contains at least one autotransformer, while the term "station" is used to refer to stations that are operated at a single voltage level. This distinction does not exist in French, and the term "poste" is used to refer to both types of facilities. Therefore, the French version of the standards only uses the term "poste" to translate the terms "station" and "substation". Thus, the terminology discussion on the use of these terms included in the section "Guidelines and technical documents" of the CIP-002-5.1 standard (p.29) could not be translated literally.

6. APPLICABILITY

All CIP version 5 standards (including CIP-010-1 and CIP-011-1) cover the same set of functions and facilities.

Applicable entities:

- Balancing Authority
- Distribution Provider²
- Generator Operator
- Generator Owner
- Interchange Coordinator or Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Applicable facilities:

- All Bulk Electric System (BES) facilities
- Facilities specific to the Distribution Provider²

Exemptions:

Refer to the "Applicability" section of each specific standard for these exemptions.

7. PROVISIONS SPECIFIC TO QUÉBEC (APPENDIX QC)

The CIP standards apply only to facilities of the main transmission system (RTP) and facilities specified in the standards specific to the Distribution Provider.

² See section "Applicability" in the CIP standards for details concerning the applicability of the Distribution Providers

8. PROPOSED EFFECTIVE DATES

The period granted to US entities upon approval of this standard in the United States was 24 months for BES Cyber Systems categorized as having a medium and high impact and 36 months for low impact systems. The enforcement date was set to April 1 2016 and 2017.

The effective dates proposed for Quebec reflect the fact that an entity possesses or not critical assets under Version 1 of the CIP standards adopted by the Régie.

Entity	Proposed effective date in Québec		Justification
	Medium and High Impact	Low Impact	
Entities covered by Version 1 of the CIP standards adopted by the Régie	2016-04-01	2017-04-01	Standardization of practices with other jurisdictions.
Entities exempt from the application of the Version 1 CIP standards under specific provisions associated to these standards	2017-04-01	2018-04-01	Allow time for the implementation of the CIP version 5 standards for entities which were exempted from the application of CIP version 1.

9. PRELIMINARY ASSESSMENT OF THE IMPACT

This section provides a preliminary assessment performed by the Coordinator of the monetary impact of the standards. Note that the framework for implementing the CIP standards implies, firstly, the identification and categorization of electronic systems according to the CIP-002 standard. An entity with no identified systems under this standard will not have to meet standards CIP-003 through CIP-011. The impact on these entities would be zero for these standards.

Impact summary

Standard	Implementation			Maintenance and Compliance Monitoring		
	Low	Medium	High	Low	Medium	High
CIP-002-5.1		X			X	
CIP-003-5			X			X
CIP-004-5.1			X			X
CIP-005-5			X			X
CIP-006-5			X			X
CIP-007-5			X			X
CIP-008-5			X			X
CIP-009-5			X			X
CIP-010-1			X			X
CIP-011-1			X			X

Legend:

Low:	Normal industry practice or standard involving minor adjustments to processes or practices in place.
Moderate:	Changes that require an allocation of certain material, human or financial resources to implement, maintain and monitor compliance of the proposed standard.
High:	Changes that require significant provision and allocation of material, human or financial resources to implement, maintain and monitor compliance of the proposed standard.

10. FINAL IMPACT ASSESSMENT

This section is to be completed upon reception of the impact assessment forms and at the end of the consultation process prior to the filing of the standards with the Régie de l'énergie.