
Project QC-2017-01

**Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6,
CIP-009-6, CIP-010-2 and CIP-011-2**

Critical Infrastructure Protection

1. ASSESSMENT OF RELEVANCE

The technology to operate interconnected power systems has evolved considerably over the years. Power system reliability is dependent on computer components, sophisticated smart devices and a new generation of communications networks to minimize potential failures.

However, these technologies also come with increased risk of cyber attacks that could threaten the integrity of the North American transmission grid. Every day, the media reports major incidents involving facilities and equipment belonging to electric power suppliers around the world.

Critical infrastructure is clearly under threat from increasingly frequent and highly sophisticated cyber attacks. Due to the interconnectedness of bulk power systems, hackers could cause cascading infrastructure outages and threaten public safety. Such attacks could have significant financial cost.

Therefore, the adoption and continuous evolution of cyber security standards is needed to protect interconnected power systems from potential threats. NERC's Project 2014-02 CIP Version 5 Revisions came from the need to clarify and update these standards in light of the cyber environment. It represents a broadening of some Version 5 requirements.

Adoption of these standards developed in this revision project by FERC in Orders 791 and 791a updated the CIP cyber security standards, which is needed to protect interconnected power systems from potential threats. These standards, version 6 of the CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2 standards are an improvement over the CIP Version 5 standards adopted by the Régie de l'énergie on July 29, 2016 (D-2016-119).

In general, the scope of the new CIP standards is similar, and the CIP Version 6 standards bring a number of improvements:

- Clarification of some vague terms that were open to interpretation
- Modification of the wording of CIP-003-6 Requirement 1 to incorporate one or more cyber security policies
- Addition of Transient Cyber Assets to the content of cyber security training programs in standard CIP-004-6
- Restriction of physical access to cabling and other nonprogrammable communication components in standard CIP-006-6

- Protection of physical ports on Protected Cyber Assets and nonprogrammable communication components in standard CIP-007-6
- Modification of CIP-010-2, Requirement 4 regarding Cyber Assets and Removable Media.
- Optimization of the French translation

There are no changes to note with regards to risk categorization (Low, Middle, High) or the risk mitigation life cycle (implement, assess, monitor and update) in the Version 6 CIP Standards.

The major changes made by FERC are summarized in the table below. Tables 11.1 to 11.7 compare Version 5 and Version 6 of Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-009-6, CIP-010-2 and CIP-011-2.

Requirement	Description and reason for change	Change
17 CIP V5 requirements	Removed the expression “detect, assess and correct”, which was found to be vague and subject to interpretation.	Text deleted
CIP-003-6, R1	To incorporate a cyber security policy or policies for low impact BES Cyber Systems, the main requirement language was modified. The expressions “for its high impact or medium impact BES Cyber Systems” and “for its assets identified in CIP-002 containing Low Impact BES Cyber Systems, if any.” were added to qualify the sub-requirements. CIP-003-6, Attachment 1 lists the components that must be covered by the Cyber Security plans for its low impact BES Cyber Systems.	Requirement expanded
CIP-004-6, R2, Part 2.1.9	Addition of Transient Cyber Assets (such as laptops) and Removable Media (such as USB thumb drive, CD, etc.) to the content of the Responsible Entity’s cyber security training programs. The training must cover the cyber security risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with Transient Cyber Assets, and with Removable Media.	Requirement expanded
CIP-006-6, R1.10	Restriction of physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.	New requirement
CIP-007-6, R1, Part 1.2	Protection of physical ports on Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter.	Requirement expanded

Requirement	Description and reason for change	Change
CIP-010-2, R4	The Standard Drafting Team used Attachment 1 of the standard rather than tables for transitory assets. It therefore modified Requirement R4 to “implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.” CIP-010-2, Attachment 1 lists the components that must be addressed by the Cyber Security plans for Transient Cyber Assets and Removable Media.	New requirement

2. PREREQUISITES TO ADOPTION

Adoption of the proposed definitions in the following section.

3. MODIFICATIONS TO OTHER STANDARDS OR GLOSSARY DEFINITIONS

The following additions, modifications and retirements shall enter into force with the proposed standards.

3.1. Standards or requirements to retire on the effective date:

Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1.

3.2. Definitions to add to glossary:

Term	Acronym	Definition
Low Impact BES Cyber System Electronic Access Point	LEAP	<p>A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.</p> <p>(Point d'accès électronique de système électronique BES à impact faible)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>
Low Impact External Routable Connectivity	LERC	<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 System 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 Cyber Assets used or owned by: 1) the Responsible Entity, 2) employees, or 3) vendors, contractors, or consultants. Remote interactive access does not include system-to-system process communications.</p> <p>(Connectivité externe routable à impact faible)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>

Term	Acronym	Definition
Removable Media	RM	<p>Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to: floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.</p> <p>(Support d'information de stockage)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>
Transient Cyber Asset	TCA	<p>A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.</p> <p>(Actif électronique transitoire)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>

3.3. Definitions to modify in glossary:

Term	Acronym	Definition
BES Cyber Asset	BCA	<p><u>New definition:</u></p> <p>A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its required operation, misoperation, 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.</p> <p><u>Old definition:</u></p> <p>A Cyber Asset that if rendered unavailable, degraded or misused would, within 15 minutes of its required operation, misoperation, 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</p>

		<p>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>(Actifs électroniques BES)</p> <p><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>
Protected Cyber Asset	PCA	<p><u>New definition:</u></p> <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.</p> <p><u>Old definition:</u></p> <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><small>Source: Glossary of Terms Used in NERC Reliability Standards</small></p>

3.4. Definitions to remove from glossary:

No change

4. CHANGES TO THE REGISTER OF ENTITIES SUBJECT TO RELIABILITY STANDARDS

The proposed standards require no change to the register of entities.

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

The English version of the standards uses the terms “stations” and “substations” to designate a group of transmission equipment located in a single location. The term “substation” is frequently used in the industry to designate a location that contains at least one autotransformer, while the term “station” is used for locations that are operated at a single voltage. This distinction does not exist in French, and the term “poste” is used for both facility types. Consequently, the French version of the standards uses the term “poste” to translate the terms “station” and “substation”.

6. APPLICABILITY

All CIP Version 6 standards apply to the same set of functions and facilities.

Functions covered:

- Balancing Authority
- Generator Operator
- Generator Owner
- Interchange Authority
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Facilities covered:

- All Bulk Electric System (BES) facilities
- Specific distributor facilities¹

Exemptions:

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

7. SPECIFIC PROVISIONS FOR QUÉBEC (QC ANNEXES)

CIP standards apply only to Main Transmission System (MTS) facilities and the Distributor facilities specified in the standards.

In addition, the Coordinator renewed the specific provision of version 5, accepted by the Régie de l'énergie in its decision D-2015-119, which exempts certain power stations and their elevators, as follows:

Additional exemptions

The following are exempt from this standard:

- Generation facilities with a rated output of 300 MVA or less, unless they include one or several generating units capable of being islanded within a neighboring system
- Step-up substations of generation facilities identified in the preceding point.

8. PROPOSED EFFECTIVE DATES

The effective dates set for US entities when these standards were approved vary by standard and their respective requirements. The proposed effective dates for Québec take into account whether an entity already has critical assets under version 1 of the CIP standards adopted by the Régie:

¹ See the Applicability section in the CIP standards for applicability details for Distributors

Standard	Entity	Effective date in the United States	Proposed effective date in Québec		Reason
			Medium and High Impact	Low Impact	
<ul style="list-style-type: none"> CIP-003-6 CIP-003-6, R1, Part 1.1 CIP-004-6 CIP-006-6 CIP-006-6, R1, Part 1.10 (High Impact and Medium Impact BES Cyber Systems at Control Centres) CIP-007-6 CIP-009-6 CIP-010-2 CIP-011-2 	Entities governed by Version 1 CIP Standards approved by the Régie.	2016-07-01	2017-07-01	2017-07-01	Standardize practices with the other jurisdictions.
	Entities exempted from the application of Version 1 of the CIP Standards under the specific provisions of those standards.		2018-10-01	2019-10-01	Provide time needed to implement Version 6 CIP Standards to entities that were exempt under Version 1
	For entities that have generation facilities for industrial use		April 1, 2019	April 1, 2020	Give the necessary time to implement version 6 of the CIP standards to entities exempted from the application of version 1.
<ul style="list-style-type: none"> CIP-003-6, R1, Part 1.2 CIP-003-6, R2 CIP-003-6, Attachment 1, Sect. 1 CIP-003-6, Attachment 1, Sect. 4 CIP-006-6, R1, Part 1.10 (High Impact and Medium Impact BES Cyber Systems at Control Centres) 	Entities governed by Version 1 CIP Standards approved by the Régie.	2017-04-01	2017-07-01	2017-07-01	Standardize practices with the other jurisdictions.
	Entities exempted from the application of Version 1 of the CIP Standards under the specific provisions of those standards.		2018-10-01	2019-10-01	Provide time needed to implement Version 6 CIP Standards to entities that were exempt under Version 1

Standard	Entity	Effective date in the United States	Proposed effective date in Québec		Reason
			Medium and High Impact	Low Impact	
<ul style="list-style-type: none"> CIP-007-6, R1, Part 1.2 (for PCA and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter for Medium or High Impact BES Cyber Systems) CIP-010-2, R4 	For entities that have generation facilities for industrial use		April 1, 2019	April 1, 2020	Give the necessary time to implement version 6 of the CIP standards to entities exempted from the application of version 1.
<ul style="list-style-type: none"> CIP-003-6, Attachment 1, Sect. 2 CIP-003-6, Attachment 1, Sect. 3 CIP-003-6, Attachment 1, Sect. 2 CIP-003-6, Attachment 1, Sect. 3 	Entities governed by Version 1 CIP Standards approved by the Régie.	2018-09-01	2018-09-01	2018-09-01	Standardize practices with the other jurisdictions.
	Entities exempted from the application of Version 1 of the CIP Standards under the specific provisions of those standards.		2018-10-01	2019-10-01	Provide time needed to implement Version 6 CIP Standards to entities that were exempt under Version 1
	For entities that have generation facilities for industrial use		April 1, 2019	April 1, 2020	Give the necessary time to implement version 6 of the CIP standards to entities exempted from the application of version 1.

The Coordinator intends to request the suspension of the effective date of 1 October 2017 of the CIPv5 requirements for the low-impact BES electronic systems currently covered, as ordered by the Régie in its decisions D-2016-119 and D -2016-138.

9. PRELIMINARY IMPACT ASSESSMENT

This section presents the Coordinator's preliminary assessment of the financial impact of the standards. Note that the framework for applying the CIP standards implies the prior identification and categorization of BES Cyber Systems in accordance with standard CIP-002. An entity with no identified applicable systems is not required to comply with Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2. There will therefore be no impact to these entities.

Impact Overview *

Standard	Implementation			Compliance monitoring		
	Low	Moderate	High	Low	Moderate	High
CIP-003-6		X			X	
CIP-004-6		X			X	
CIP-006-6		X			X	
CIP-007-6		X			X	
CIP-009-6		X			X	
CIP-010-2		X			X	
CIP-011-2		X			X	

Legend:

Low:	Normal industry practice that only requires minor adjustments to existing processes or practices.
Moderate:	Change that requires allocation of some physical, human or financial resources to implement, maintain or monitor compliance with the proposed standard.
High:	Change that requires allocation of significant physical, human or financial resources to plan, implement, maintain or monitor compliance with the proposed standard.

* The Coordinator's evaluation is based on the differences between the version 5 and version 6 of the CIP standards.

10. FINAL IMPACT ASSESSMENT

This section shall be completed upon receipt of the impact assessment forms and at the conclusion of the consultation process prior to filing of reliability standards with the Régie de l'énergie.

11. CIP V5 vs CIP V6 Cross-reference table

11.1.CIP-003-6 – Cyber Security – Security Management Controls

CIP-003-5	CIP-003-6	Description and justification of change
R1	R1	To incorporate a cyber security policy or policies for low impact BES Cyber Systems, the main requirement language was modified. The expression “for its High or Medium Impact BES Cyber Systems” was removed with the addition of the new Parts. See Parts 1.1 and 1.2 below for the justification of the change.
	R1.1	The phrase “for its High or Medium Impact BES Cyber Systems” was added to qualify the new Parts below.
R1.1	R1.1.1	Parts 1.1 to 1.9 became 1.1.1 to 1.1.9, and the expression above was added to CIP-003-6, Part 1.1.
R1.2 to R1.9	R1.1.2 to R1.1.9	No change
	R1.2	The expression “for its assets identified in CIP-002 containing Low Impact BES Cyber Systems, if any.” was added to qualify the sub-requirements below.
R2	R2	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed. Furthermore, as the Standard Drafting Team (SDT) opted to use Attachment 1 rather than tables, requirement R2 was modified to read: “shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.”
R2.1	R1.2.1	The Part addressing the cyber security awareness that must be covered by one or more documented cyber security plan(s) was moved to CIP-003-6, R1, Part 1.2.1.
R2.2	R1.2.2	The Part addressing the physical security measures that must be covered by one or more documented cyber security plan(s) was moved to CIP-003-6, R1, Part 1.2.2.

CIP-003-5	CIP-003-6	Description and justification of change
R2.3	R1.2.3	The Part addressing the electronic access control that must be covered by one or more documented cyber security plan(s) was moved to CIP-003-6, R1, Part 1.2.3. Furthermore, the SDT modified the “external routable protocol connections” as the SDT proposed the new term “Low Impact External Routable Connectivity”.
R2.4	R1.2.4	Part 2.4 addressing the incident response to a Cyber Security Incident that must be covered by one or more of the documented cyber security policies was moved to CIP-003-6, R1, Part 1.2.4.
	Attachment 1	CIP-003-6, Attachment 1 lists the components that must be covered by the Cyber Security plans for its low impact BES Cyber Systems. The attachment is in response to FERC Order No. 791 regarding the lack of objective criteria for the protection of low impact assets.
R3	R3	No change
R4	R4	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.

11.2.CIP-004-6 – Cyber Security – Personnel & Training

CIP-004-5.1	CIP-004-6	Description and justification of change
R1	R1	No change
R1.1	R1.1	No change

CIP-004-5.1	CIP-004-6	Description and justification of change
R2.1	R2.1	No change
R2.1.1 to R2.1.8	R2.1.1 to R2.1.8	No change
R2.1.9	R2.1.9	To respond to the FERC Order No. 791 directives regarding transient devices, the SDT has added Transient Cyber Assets and Removable Media as contents that must be included in a Responsible Entity's cyber security training programs. The training must address cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with Transient Cyber Assets, and with Removable Media.
R2.2	R2.2	No change
R2.3	R2.3	No change
R3	R3	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression "to identify, assess and correct deficiencies" was removed.
R3.1 to R3.5	R3.1 to R3.5	No change
R4	R4	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression "to identify, assess and correct deficiencies" was removed.
R4.1 to R4.4	R4.1 to R4.4	No change
R5	R5	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression "to identify, assess and correct deficiencies" was removed.
R5.1 to R5.5	R5.1 to R5.5	No change

11.3.CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems

<i>CIP-006-5</i>	<i>CIP-006-6</i>	Description and justification of change
R1	R1	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R1.1 to R1.9	R1.1 to R1.9	No change
	R1.10	In response to the FERC Order No. 791 directive to protect the nonprogrammable components of communication networks, the SDT has added a new Requirement R1, Part 1.10 to restrict physical access to cabling and other nonprogrammable components used for communication between applicable Cyber Assets within the same Electronic Security Perimeter. The entity has three other mechanisms to adequately protect these networks: encryption of the data transmitted by these cables and components, monitoring the status of the communication link and issuing an alarm in response to detected communication failures, an equally effective logical protection.
R2	R2	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R2.1 to R2.3	R2.1 to R2.3	No change
R3	R3	No change
E3.1	E3.1	No change

11.4.CIP-007-6 – Cyber Security – Systems Security Management

CIP-007-5	CIP-007-6	Description and justification of change
R1	R1	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R1.1	R1.1	No change
R1.2	R1.2	The applicable systems column was modified to include the Protected Cyber Assets and nonprogrammable communication components located inside both a Physical Security Perimeter and an Electronic Security Perimeter. The protection against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media for these additions addresses the communication networks directive from GERC Order No. 791. Removable Media was capitalized in the requirement because it is newly defined.
R2	R2	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R2.1 to R2.4		No change
R3	R3	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R3.1 to R3.3	R3.1 to R3.3	No change
R4	R4	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R4.1 to R4.4	R4.1 to R4.4	No change
R5	R5	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R5.1 to R5.5	R5.1 to R5.5	No change
R6	R6	No change
R7	R7	No change

11.5.CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems

CIP-009-5	CIP-009-6	Description and justification of change
R1	R1	No change
R1.1 to R1.5	R1.1 to R1.5	No change
R2	R2	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R2.1 to R2.3	R2.1 to R2.3	No change
R3	R3	No change
R3.1 to R3.2	R3.1 to R3.2	No change

11.6.CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments

CIP-010-1	CIP-010-2	Description and justification of change
R1	R1	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
	R4	In response to FERC Order No. 791 regarding transient assets, the SDT changed its approach, using Attachment 1 rather than tables. It therefore modified Requirement R4 to “implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.”
	Attachment 1	CIP-010-2, Attachment 1 lists the components that must be addressed by the Cyber Security plans for Transient Cyber Assets and Removable Media. The attachment is in response to FERC Order No. 791 regarding the risks associated with transient assets.

11.7.CIP-011-2 – Cyber Security – Information Protection

CIP-011-1	CIP-011-2	Description and justification of change
R1	R1	In response to FERC Order No. 791 to remove ambiguous language from the requirement, the expression “to identify, assess and correct deficiencies” was removed.
R1.1 to R1.2	R1.1 to R1.2	No change
R2	R2	No change
R2.1 to R2.2	R2.1 to R2.2	No change