
Project QC-2019-05

CIP-005-6 – Cyber Security - Electronic Security Parameter(s), CIP-010-3 – Cyber Security - Configuration Change Management and Vulnerability Assessments, and CIP-013-1 – Cyber Security - Supply Chain Risk Management

1. OVERVIEW OF THE STANDARDS

1.1. Applicability

The CIP-005-6, CIP-010-3 and CIP-013-1 standards apply to the same set of functions and facilities:

Functions covered:

- Certain Distribution Providers
- Generator Operator (GOP)
- Generator Owner (GO)
- Balancing Authority (BA)
- Interchange Authority
- Reliability Coordinator (RC)
- Transmission Operator (TOP)
- Transmission Owner (TO)

Facilities covered:

- RTP facilities that meet the criteria established in the “Applicability” section.
- Specific facilities for Distribution Providers¹

1.2. Purpose of the Reliability Standard

The purpose of the supply chain management requirements is to protect aspects of the supply chain that are within the control of the responsible entities and apply to BES Cyber Systems categorized as high or medium impact according to the identification and categorization process required by CIP-002-5.1a. The supply chains for information and communications technology and industrial control systems present risks to the BES by providing potential opportunities for the introduction of cybersecurity vulnerabilities.

The new CIP-013-1 standard as well as modifications to the CIP-005-6 and CIP-010-3 standards require applicable entities to develop and implement a plan that addresses, at a minimum four objectives as defined in FERC Order 829:

- Software integrity and authenticity;
- Vendor remote access;
- Information system planning
- Vendor risk management and procurement controls

¹ See section “Applicability” in the CIP standards for details concerning the applicability of the Distribution Providers

The supply chain management requirements are aimed at the protection of aspects of the supply chain that are within the control of the responsible entities and apply to BES Cyber Systems categorized as high or medium impact according to the identification and categorization process required by CIP-002-5.1a.

1.3. Regulatory Context

The Régie de l'énergie (hereinafter "the Régie") adopted CIP-005-5 in Decision D-2016-119² and adopted CIP-010-2 in Decision D-2017-117³ and have been in effect since January 1, 2017 and January 1, 2018, respectively.

Adopted by the NERC Board of Trustees on August 10, 2017 and subsequently approved by FERC on October 28, 2018 in Order No. 850,⁴ the CIP-005-6, CIP-010-3 and CIP-013-1 standards will come into effect in the United States on July 1st, 2020.

1.4. Specific Provisions for Québec

The Reliability Coordinator (hereinafter called "the Coordinator") is proposing to renew the Québec specific provisions, particularly in the applicability and the specific provisions already adopted by the Régie in its ruling D-2016-119, which exempts certain facilities and their step-up substation. The standards apply to the facilities of the Main Transmission System (RTP) and to the facilities specified for the Distribution Provider. In addition, the following specific provisions apply:

- Any generating facility and its step-up substation that meets the two following conditions (1) the nameplate capacity of the facility is 300 MVA or less, and (2) no unit of the facility can be synchronized with a neighbouring system are exempt from the standards.
- Step-up substations of generating facilities identified in the preceding point are exempt.

1.5. Proposed Effective Dates

The CIP-005-6, CIP-010-3 and CIP-013-1 standard will come into effect in the United States on July 1, 2020. The NERC Implementation Plan⁵ allows for a period of 18 months between regulatory approval and the implementation of the standard. The initial review and approval of supply chain cyber security risk management plans by the CIP Senior Manager in Requirement R3 must be completed on or before the effective date of CIP-013-1.

In Québec, the Reliability Coordinator proposes an effective date which is 18 months beyond the adoption of the CIP-005-6, CIP-010-3 and CIP-013-1 standards by the Régie.

1.6. Standards or Requirements to Retire

Standards CIP-005-5 and CIP-010-2 are to be retired when CIP-005-6, CIP-010-3 and CIP-013-1 come into effect.

² Régie de l'Énergie, Decision D-2016-119, consulted online on August 13, 2019, at: http://publicsde.regie-energie.qc.ca/projets/335/DocPri/R-3947-2015-A-0022-Dec-Dec-2016_07_29.pdf

³ Régie de l'Énergie, Decision D-2017-117, consulted online on August 13, 2019, at: http://publicsde.regie-energie.qc.ca/projets/408/DocPri/R-4005-2017-A-0009-Dec-Dec-2017_10_31.pdf

⁴ FERC, Order No. 850, consulted online on August 13, 2019, at <https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf>

⁵ NERC Implementation Plan, consulted online on August 13, 2019, at: https://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/Implementation_Plan_Clean_07_1117.pdf

1.7. Modifications to the Glossary

The coming into effect of the standards is contingent upon the changes to the definitions of the terms Remedial Action Scheme and Special Protection System as requested to the Régie in docket R-4070-2018.

2. ASSESSMENT OF RELEVANCE

Subsequent to FERC Order No. 829⁶, NERC developed a reliability standard that addresses supply chain management for industrial control system hardware, software, and computing and networking services that impact the Bulk Electric System (BES) operations. Modifications made to CIP-005-5 address FERC's concerns regarding vendor remote access. Regarding CIP-010-2, revisions address FERC's concerns associated with software integrity and authenticity. These modifications are as relevant in Québec as elsewhere in North America.

In accordance with the agreement made in 2009 between the Régie, NERC and the NPCC and with the authorization of the Québec government,⁷ this standard was developed and approved by external agencies for North America, including Québec. In the opinion of the Reliability Coordinator, this standard is relevant for system reliability in Québec and the standard contributes to harmonization with neighboring systems.

3. PRELIMINARY IMPACT ASSESSMENT

This section presents the Reliability Coordinator's preliminary impact assessment.

CIP-005-6	Low	Moderate	High
Implementation of the standard		X	
Enforcement of the standard		X	
Compliance monitoring		X	

CIP-010-3	Low	Moderate	High
Implementation of the standard		X	
Enforcement of the standard		X	
Compliance monitoring		X	

CIP-013-1	Low	Moderate	High
Implementation of the standard		X	
Enforcement of the standard		X	
Compliance monitoring		X	

Legend:

⁶ FERC, Order No. 829, consulted online on August 13, 2019, at : <https://www.ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf>

⁷ Agreement entered into in accordance with Order-in-Council 443-21009 dated April 8, 2019.

- 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 the proposed standard, maintain it or monitor its compliance.
- High:** Change that requires allocation of significant physical, human or financial resources to plan and implement the proposed standard, maintain it or monitor its compliance.

4. 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.