

---

## Project QC-2021-08

### **Standards CIP-005-7 – Cyber Security – Electronic Security Perimeter(s), CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments and CIP-013-2 – Cyber Security – Supply Chain Risk Management**

---

#### 1.1. Applicability

The reliability standards proposed for adoption (CIP-005-7, CIP-010-4 and CIP-013-2) apply to the following functional entities.

Standard	Functional entities
CIP-005-7	<ul style="list-style-type: none"><li>• Generator Operator (GOP)</li><li>• Generator Owner (GO)</li><li>• Balancing Authority (BA)</li><li>• Reliability Coordinator (RC)</li><li>• Transmission Operator (TOP)</li><li>• Transmission Owner (TO)</li><li>• Certain Distribution Providers (DP)</li></ul>
CIP-010-4	
CIP-013-2	

The standards drafting team of the North American Electric Reliability Corporation (NERC) has removed Interchange Coordinator or Interchange Authority from the functional entities to which standards CIP-005-7 and CIP-010-4 apply<sup>1</sup>, which is why the three standards now apply to the same functional entities.

#### 1.2. Purpose of the standards

The title and purpose of each standard covered by this request are presented below.

- **CIP-005-7 – Cyber Security – Electronic Security Perimeter(s):** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- **CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

---

1. Technical Rationale and Justification for Reliability Standard CIP-005-7, NERC (p.4/17), retrieved June 29, 2021, from [https://www.nerc.com/pa/Stand/Project201903\\_Cyber%20Security%20Supply%20Chain%20Risks/2019-03\\_CIP-005-7\\_Technical\\_Rationale\\_clean\\_10072020.pdf](https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-005-7_Technical_Rationale_clean_10072020.pdf)

- **CIP-013-2 – Cyber Security – Supply Chain Risk Management:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

### 1.3. Regulatory context

These three reliability standards replace standards CIP-005-6, CIP-010-3 and CIP-013-1, adopted by the Régie de l'énergie (the Régie) in decision D-2020-118<sup>2</sup>. Standards CIP-005-6, CIP-010-3 and CIP-013-1 will become effective in Québec on October 1, 2022.

Adopted by the NERC Board of Trustees on November 5, 2020, and approved by the Federal Energy Regulatory Commission (FERC) on March 18, 2021 (letter order, docket No. RD21-2-000)<sup>3</sup>, reliability standards CIP-005-7, CIP-010-4 and CIP-013-2 will become effective in the United States on October 1, 2022<sup>4</sup>.

The Reliability Coordinator (the Coordinator) files herewith standards CIP-005-7, CIP-010-4 and CIP-013-2 of NERC Project 2019-03 (Supply Chain Risk management)<sup>5</sup>. This is the only submission for this project. The purpose of the three reliability standards is to respond to the directive issued by FERC in order No. 850<sup>6</sup> to modify the supply chain cyber security risk management reliability standards for BES Cyber Systems. FERC directed NERC to submit modifications to address Electronic Access Control and Monitoring Systems (EACMS), specifically those systems that provide electronic access control and monitoring to high and medium impact BES Cyber Systems. In its report of May 17, 2019<sup>7</sup>, NERC recommends revising the supply chain cyber security risk management reliability standards to include within their scope Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems<sup>8</sup>. In other words, the purpose of project 2019-03<sup>9</sup> is to extend the applicability of reliability standards CIP-005-7, CIP-010-4 and CIP-013-2 to include EACMS and PACS.

### 1.4. Special provisions for Québec

The Coordinator proposes carrying over the Québec-specific provisions (including applicability) in the preceding versions of the reliability standards (standards CIP-005-6, CIP-010-3 and CIP-013-1) already adopted by the Régie in decision D-2020-118, which exempted certain generating stations and their step-up substations.

The first such special provision concerns the applicability of the standard:

---

2. Régie decision D-2020-118, docket R-4117-2020, retrieved June 29, 2021, from [http://publicsde.regie-energie.qc.ca/projets/536/DocPri/R-4117-2020-A-0011-Dec-Dec-2020\\_09\\_10.pdf](http://publicsde.regie-energie.qc.ca/projets/536/DocPri/R-4117-2020-A-0011-Dec-Dec-2020_09_10.pdf)

3. FERC letter order in docket RD21-2-000, retrieved July 26, 2021, from [https://elibrary.ferc.gov/eLibrary/filelist?accession\\_num=20210318-3030](https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20210318-3030).

4. Standards subject to a future coming into force on the NERC website, retrieved June 16, 2021, from <https://www.nerc.net/standardsreports/standardssummary.aspx>.

5. NERC Project 2019-03, retrieved June 29, 2021, from [https://www.nerc.com/pa/Stand/Pages/Project2019-03Cyber\\_securitySupplyChain-Risks.aspx](https://www.nerc.com/pa/Stand/Pages/Project2019-03Cyber_securitySupplyChain-Risks.aspx)

6. FERC Order No. 850, retrieved June 29, 2021, from <https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf>

7. NERC report, *Cyber Security Supply Chain Risks, Staff Report and Recommended Actions*, retrieved June 29, 2021, from [https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20\(20190517\).pdf](https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf)

8. Standard Authorization Request, retrieved June 29, 2021, from [https://www.nerc.com/pa/Stand/Project201903\\_Cyber%20Security%20Supply%20Chain%20Risks/SAR%20Supply%20Chain\\_July2019.pdf](https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/SAR%20Supply%20Chain_July2019.pdf)

9. NERC Project 2019-03, retrieved June 29, 2021, from [https://www.nerc.com/pa/Stand/Pages/Project2019-03Cyber\\_securitySupplyChain-Risks.aspx](https://www.nerc.com/pa/Stand/Pages/Project2019-03Cyber_securitySupplyChain-Risks.aspx)

This standard applies only to facilities of the Main Transmission System (RTP) and to designated distribution provider facilities. When applying this standard, any reference to the terms Bulk Electric System or BES shall be replaced by the terms Main Transmission System or RTP, respectively.

The Coordinator is of the opinion that this special provision is still applicable because the scope of application determined by the Régie for most Reliability Standards in Québec is the RTP.

The Coordinator proposes that the following exemptions be carried over:

The following are exempt from this standard:

- Any generation facility that meets both of the following conditions: (1) the rated power of the facility is 300 MVA or less and (2) none of the facility's generating units can be synchronized with a neighboring system
- Step-up substations of generating facilities that meet the conditions mentioned above

The Coordinator is of the opinion that the special provision with respect to the additional exemptions is still applicable in the new versions of standards CIP-005, CIP-010 and CIP-013 because the exemption criteria mentioned above reference low-impact facilities.

### 1.5. Proposed effective dates

The implementation plan for NERC Project 2019-03<sup>10</sup> proposes that Reliability Standards CIP-005-7, CIP-010-4 and CIP-013-2 become effective on the first day of the first calendar quarter that is 18 months beyond the date of their regulatory approval.<sup>11</sup> The three Reliability Standards will become effective in the United States on October 1, 2022.

The Coordinator considers the Régie's requirement that standards come into force on the first day of a calendar quarter<sup>12</sup> with at least 60 days<sup>13</sup> between the date of the standard's adoption and its effective date is compliant with NERC's implementation plan.

Given the importance of having standardized practices, with effective mandatory standards harmonized with the United States, the Coordinator proposes that the three reliability standards come into effect on the first day of the first calendar quarter that is 18 months beyond their adoption by the Régie.

### 1.6. Standards to retire

Reliability standards CIP-005-6, CIP-010-3 and CIP-013-1 must be retired as soon as Reliability Standards CIP-005-7, CIP-010-4 and CIP-013-2 respectively take effect.

---

10. NERC Implementation Plan, Project 2019-03, retrieved June 16, 2021, from [https://www.nerc.com/pa/Stand/Project201903\\_Cyber%20Security%20Supply%20Chain%20Risks/2019-03\\_Implementation\\_Plan\\_clean\\_10072020.pdf](https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Implementation_Plan_clean_10072020.pdf).

11. NERC Implementation Plan, Project 2019-03 (p.2/4), retrieved June 16, 2021, from [https://www.nerc.com/pa/Stand/Project201903\\_Cyber%20Security%20Supply%20Chain%20Risks/2019-03\\_Implementation\\_Plan\\_clean\\_10072020.pdf](https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_Implementation_Plan_clean_10072020.pdf)

12. In decision [D-2015-168](#), the Régie set the effective date of standards as the first day of the calendar quarter following the date of adoption of the standard.

13. In decision [D-2016-011](#), the Régie set a minimum of 60 days between adoption of a standard and its effective date.

## 1.7. Changes to the Glossary

No changes to the Glossary.

## 2. ASSESSMENT OF RELEVANCE

In the United States, FERC issued a directive in Order No. 850<sup>14</sup> that Electronic Access Control and Monitoring Systems (EACMS), more specifically those that control and monitor electronic access to medium and high impact BES Cyber Systems, be included in the scope of supply chain cyber security risk management standards. In effect, FERC determined that there remains a significant cyber security risk associated with the supply chain for BES Cyber Systems because the approved reliability standards do not address electronic access control and monitoring.<sup>15</sup> The standards proposed herein address FERC's directive.

EACMS play a significant role in the protection of medium and high impact BES Cyber Systems. Once an EACMS is compromised, an attacker could more easily enter the security perimeter and effectively control the BES Cyber System or protected cyber asset<sup>16</sup>.

NERC has added to the FERC directive, proposing that Physical Access Control Systems (PACS) providing physical access control to high and medium impact BES Cyber Systems be included in the scope of supply chain cyber security risk management standards, even though a physical presence is required in order to exploit the BES Cyber System vulnerability created by a remotely compromised PACS. The risk posed to BES Cyber System reliability by a compromised, misused, degraded or unavailable PACS warrants their inclusion as applicable Cyber Assets<sup>17</sup>.

Basically, this means adding requirement R3 to Reliability Standard CIP-005-7 and adding EACMS and PACS to the requirements already present in Reliability Standards CIP-010-4 and CIP-013-2. Requirement R3 was added in order to have one or more methods to determine and terminate authenticated vendor-initiated remote connections and control the ability to reconnect<sup>18</sup>.

For reliability standards CIP-010-4 and CIP-013-2, a reference to EACMS and PACS was added to each of the requirements.

As mentioned in the letter order in docket No. RD21-2-000<sup>19</sup>, FERC is of the opinion that including EACMS and PACS in Reliability Standards CIP-005-7, CIP-010-4 and CIP-013-2 improves BES system reliability while

---

14. FERC Order No. 850, retrieved June 29, 2021, from

<https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf>

15. FERC Order No. 850 (p.3), retrieved June 29, 2021, from

<https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf>

16. FERC Order No. 850 (p.4), retrieved June 29, 2021, from

<https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf>

17. NERC Technical Rationale and Justification for Reliability Standard CIP-005-7, retrieved June 29, 2021, from

[https://www.nerc.com/pa/Stand/Project201903\\_Cyber%20Security%20Supply%20Chain%20Risks/2019-03\\_CIP-005-7\\_Technical\\_Rationale\\_clean\\_10072020.pdf](https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-005-7_Technical_Rationale_clean_10072020.pdf)

18. NERC Summary of Changes, retrieved August 12, 2021, from

[https://www.nerc.com/pa/Stand/Project201903\\_Cyber%20Security%20Supply%20Chain%20Risks/2019-03\\_CIP-005-7\\_Summary\\_of\\_Changes\\_10072020.pdf](https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-005-7_Summary_of_Changes_10072020.pdf)

19. FERC letter order in docket No. RD21-2-000, retrieved June 16, 2021, from

[https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Supply%20Chain%20Risk%20Management\\_final.pdf](https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Supply%20Chain%20Risk%20Management_final.pdf)

maintaining the security objectives mentioned in the original versions of the supply chain cyber security risk management standards.

In addition, the New Brunswick Energy and Utilities Board<sup>20</sup> has undertaken project No. 498 to address NERC Project 2019-03, though the Ontario Energy Board has not yet begun addressing this NERC project.

The Coordinator is of the opinion that standards CIP-005-7, CIP-010-4 and CIP-013-2 are relevant for Québec because the same weakness in supply chain cyber security risk management exists in Québec, that is, a malicious attack could be made via the EACMS and PACS that would directly impact the BES Cyber Systems by disturbing associated activities. The proposed standards correct this weakness.

Given the information outlined above regarding standards CIP-005-7, CIP-010-4 and CIP-013-2, and given that these standards were developed by recognized North American authorities and in compliance with the agreement signed in 2009 by the Régie, NERC and the NPCC with the authorization of the Government of Québec<sup>21</sup>, the Coordinator is of the opinion that standards CIP-005-7, CIP-010-4 and CIP-013-2 contribute to the reliability of the Québec grid.

### 3. PRELIMINARY IMPACT ASSESSMENT

This section provides the Reliability Coordinator's preliminary assessment of the impact on all Québec entities.

The registered entities already have mechanisms in place to meet the requirements of the new versions of standards CIP-005 and CIP-013, which is why the Coordinator considers the impact to be low. The impact on registered entities of the new version of standard CIP-010, however, is considered to be moderate because there will be an increase in workload to implement, enforce and monitor compliance with the requirements of the new version, and management of the mechanism in place can be improved.

Standard	Impact		
	Implementation	Enforcement	Monitoring
CIP-005-7	Low	Low	Low
CIP-010-4	Moderate	Moderate	Moderate
CIP-013-2	Low	Low	Low

#### Legend

- Low:** Normal industry practice or standard that only requires minor adjustments to existing processes or practices.
- Moderate:** Change that requires the mobilization of some physical, human or financial resources to implement the proposed standard, enforce it or monitor its compliance.
- High:** Change that requires provision and mobilization of significant physical, human or financial resources to plan and implement the proposed standard, enforce it or monitor its compliance.

20. New Brunswick Energy & Utilities Board project No. 498, retrieved June 29, 2021, from <https://filemaker.nbeub.ca/fmi/webd/NBEUB%20Toolkit13>

21. Agreement entered into pursuant to decree No. 443-2009 issued on April 8, 2009, [https://www.nerc.com/files/NERC-Regie-NPCC\\_Agreement\\_20090508EN\\_signed.pdf](https://www.nerc.com/files/NERC-Regie-NPCC_Agreement_20090508EN_signed.pdf)

#### **4. FINAL IMPACT ASSESSMENT**

This section will be completed upon receipt of the impact assessment forms and at the conclusion of the consultation process prior to filing of the standards with the Régie.