
Project QC-2019-05

CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

1. OVERVIEW OF THE STANDARD

1.1. Applicability

Functions covered:

- Certain Distribution Providers
- Generator Operator (GOP)
- Generator Owner (GO)
- Balancing Authority (BA)
- 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 CIP-008 standard is to mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

1.3. Regulatory Context

The Régie de l'énergie (hereinafter “the Régie”) adopted CIP-008-5 and its appendix in Decision D-2016-119². The standard has been in effect since January 1, 2017.

The NERC Board of Trustees adopted CIP-008-6 on February 2, 2019. FERC subsequently approved the standards on June 20, 2019 in Docket No. RD19-3-000.³

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:

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

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 FERC, Docket No. RD19-3-000, consulted online on August 13, 2019, at <https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Docket%20No.%20RD19-3-000.pdf>

- 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-008-6 standard will come into effect in the United States on January 1, 2021. In the United States, the NERC Implementation Plan⁴ allows for a period of 18 months between regulatory approval and the implementation of the standard.

In Québec, the Reliability Coordinator proposes an effective date which is 18 months beyond the adoption of the CIP-008-6 standard by the Régie.

1.6. Standards or Requirements to Retire

The CIP-008-5 standard is to be retired when CIP-008-6 comes into effect.

1.7. Modifications to the Glossary

Modifications to the Glossary shall take effect on the effective date of CIP-008-6.

The following terms will be modified:

- Cyber Security Incident
- Reportable Cyber Security Incident

The definitions of these terms, in French and in English, are provided in the document “Modifications au Glossaire”.

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. 848⁵, NERC modified CIP-008-5 to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES).

The new CIP-008-6 standard as well as modifications to the definitions, addresses, the four elements outlined in FERC Order 848:

- Reporting of Cyber Security Incidents that compromise, or attempt to compromise an Electric Security Perimeter (ESP) or associated Electronic Access Control or Monitoring System (EACMS);
- Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;
- Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity;

⁴ 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_071117.pdf

⁵ FERC, Order No. 848, consulted online on August 13, 2019, at :

https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/E-1_Order%20No.%20848.pdf

Cyber Security Reports should be sent to Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Modifications to the standard in regards to augmenting mandatory reporting of Cyber Security Incidents, including attempts to compromise an entity's ESP or EACMS, as well as revisions to requirements R1 through R4 reflecting the addition of EACMS systems associated with High and Medium BES Cyber Systems modifications are as relevant to Québec as to the rest of 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,⁶ 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.

	Low	Moderate	High
Implementation of the standard		X	
Enforcement of the standard		X	
Compliance monitoring		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 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.

⁶ Agreement entered into in accordance with Order-in-Council 443-21009 dated April 8, 2019.