Diane Roy
Vice President, Regulatory Affairs

Gas Regulatory Affairs Correspondence
Email: gas.regulatory.affairs@fortisbc.com

Electric Regulatory Affairs Correspondence
Email: electricity.regulatory.affairs@fortisbc.com

FortisBC
16705 Fraser Highway
Surrey, B.C. V4N 0E8
Tel: (604) 576-7600
Fax: (604) 576-7074
www.fortisbc.com

August 12, 2020

British Columbia Utilities Commission
Suite 410, 900 Howe Street
Vancouver, B.C.
V6Z 2N3

Attention: Ms. Marija Tresoglavic, Acting Commission Secretary

Dear Ms. Tresoglavic:

Re: British Columbia Hydro and Power Authority (BC Hydro) Mandatory Reliability Standards (MRS) Assessment Report No. 13 (Report)

FortisBC Inc. (FBC) Response to the British Columbia Utilities Commission (BCUC) Information Request (IR) No. 1

In accordance with BCUC Order R-10-2020 setting out the Regulatory Timetable for the review of the above noted Report, FBC respectfully submits the attached response to BCUC IR No. 1.

If further information is required, please contact Joyce Martin, Manager, Regulatory Affairs at 250-368-0319.

Sincerely,

FORTISBC INC.

Original signed:

Diane Roy

Attachments

cc (email only): Registered Parties

A. RECOMMENDED EFFECTIVE DATES

1.0 Reference: Assessment of Individual Standards

Exhibit B-1, Section 5.3, Table 3, p. 22; Appendix C-3, p. 7 CIP-008-6 Recommended Effective Date

In British Columbia Hydro and Power Authority's (BC Hydro) Mandatory Reliability Standards (MRS) Assessment Report No. 13 (Report), page 22 states that FortisBC Inc.'s (FBC) "recommended effective date is 24-36 months after BCUC approval" for CIP-008-6.

On page 7 of Appendix C-3 of the Report, in the column titled "Stakeholder Comments Organizational Activities and Reliability/Suitability Impact," Standard CIP-008-6 R1 reads:

FortisBC requires additional hardware and software to address devices coming into scope. Fortis BC will also need to develop criteria to evaluate and define attempts to compromise. Ongoing costs are associated with implementing criteria as well as analyzing and reporting attempts to compromise.

FBC also applies the above comment to CIP-008-6 R2, R3 and R4.

1.1 Please elaborate on FBC's recommended 24–36 month effective date for CIP-008-6.

Response

With the increase of devices in scope and the addition of reportable incidents including "Attempts to Compromise", FBC believes 24-36 months provides appropriate time to evaluate, select, design, test, and implement the most appropriate solution(s). Please also refer to the response to BCUC IR1 1.2 which describes the minimum scope of work required to achieve compliance

The timeline also allows for the FBC MRS audit scheduled in 2021.

1.2 Please explain what types of additional hardware and software are required to become compliant with CIP-008-6.

Response

CIP-008-6 1.2.1 introduces the term "Attempts to Compromise" to the Cyber Security Incident Response Plan specification. Each occurrence of unknown network traffic on any High or Medium Impact Bulk Electric System (BES) Cyber System and their associated Electronic Access Control

and Monitoring Systems (EACMS) must be analyzed to determine if it meets the threshold as an Attempt to Compromise. The overall approach is to reduce or eliminate network traffic hitting in-scope assets either from outside the FBC network or inside the Electronic Security Perimeter (ESP) from other BES Assets.

At a minimum, new hardware firewalls, intrusion detection and prevention software, as well as analysis and possible redesign or reconfiguration of the in-scope network will be required. Any Attempt to Compromise will require reporting, therefore a thorough evaluation of hardware and software infrastructure is needed to minimize unnecessary network noise and support efficient and accurate reporting.