Sarah Walsh
Director, 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: (778) 578-3861
Cell: (604) 230-7874
Fax: (604) 576-7074
www.fortisbc.com

January 9, 2025

British Columbia Utilities Commission
Suite 410, 900 Howe Street
Vancouver, BC
V6Z 2N3

Attention: Patrick Wruck, Commission Secretary

Dear Patrick Wruck:

Re: FortisBC Energy Inc. (FEI)

Application for a Certificate of Public Convenience and Necessity (CPCN) for the Tilbury Liquefied Natural Gas Storage Expansion (TLSE) Project (Application)

FEI Reply Submissions on Confidentiality Requests

FEI writes to provide its reply to intervener comments in response to FEI's request that certain information be held confidential by the British Columbia Utilities Commission (BCUC) in perpetuity, including information that is requested to be held confidential and available only to the BCUC, pursuant to the regulatory timetable set out in Order G-324-24.

The Commercial Energy Consumers Association of British Columbia (CEC),[1] the BC Sustainable Energy Association (BCSEA)[2] and the Residential Consumer Intervener Association (RCIA)[3] provided submissions regarding FEI's confidentiality requests. CEC submits that it has no issue with FEI's proposed confidentiality requests. While BCSEA and RCIA agree with FEI that the specified information in the Supplemental Evidence and 2024 Resiliency Plan warrants confidential treatment, they want access to all of the "Restricted Confidential Information" based on signed undertakings alone.

FEI has taken care to limit redactions to the most security sensitive information, and most of the filed information – including that information most pertinent to the Application – is fully public. The remaining redacted information is highly security sensitive on its face. For the reasons noted in FEI's initial confidentiality request and elaborated below, FEI respectfully submits that there is a very compelling case for maintaining the highest level of protection over the redacted Restricted Confidential Information in the 2024 Resiliency Plan. That means limiting access to the BCUC only.

---

1 Exhibit C5-25.
2 Exhibit C2-17.
3 Exhibit C1-23.

First, as outlined in the cover letter to the 2024 Resiliency Plan, the Restricted Confidential Information is highly sensitive information that FEI submits could provide a roadmap for malicious actors to exploit if aggregated. It includes, in particular, deanonymized details about specific vulnerabilities to FEI's system, such as their locations, and particular modes of failure (hazards) that pose the most likely and most severe risk of causing significant customer outages. Put simply, the 2024 Resiliency Plan contains some of the most sensitive types of information related to a gas utility, including the examples cited by RCIA[4], and the specific de-anonymized information about each of the 58 Assessed Vulnerabilities.[5] It is clear that distribution of this information could be used to harm FEI and its customers, and therefore, should be carefully limited.

Second, while BCSEA questions the basis in the BCUC Rules of Practice and Procedure (BCUC Rules) for limiting access to the Restricted Confidential Information category to the BCUC only, Rule 24 is clear that the BCUC "may consider whether access to the confidential information may be provided to certain parties upon request" [emphasis added]. Rule 19 enables the Panel to grant a request for confidentiality "on any terms it considers appropriate". Indeed, FEI's proposed treatment of the Restricted Confidential Information is similar to that of the BCUC's Rules of Procedure for Reliability Standards in British Columbia (Order R-40-17) which contemplates a category of confidential "Restricted Information" that is subject to additional protection, including withholding the information from interveners and the public.[6] The type of security sensitive information at issue here is analogous to the Restricted Information protected in relation to electric utilities. Physical information about critical assets is the very sort of information that the BCUC limits to the BCUC only in respect of Mandatory Reliability Standards.

Third, as recognized by BCSEA,[7] FEI confined the Restricted Confidential Information to the 2024 Resiliency Plan. The majority of the specified information is not directly relevant to the BCUC's ultimate decision regarding the TLSE Project, but rather, is responsive to the BCUC's request for more analysis than what had been presented in the initial version of the Resiliency Plan filed as an appendix to the 2022 Long Term Gas Resource Plan (LTGRP). The BCUC requested a holistic plan. The 2024 Resiliency Plan provides a holistic vulnerability assessment encompassing FEI's own system and regional infrastructure, and to the extent possible, FEI has anonymized and maintained public access to information that directly supports the need for the TLSE Project. For instance:

- Interveners and the public know that AV-1, 2, 3 and 54 collectively comprise T-South;
- Interveners and the public can see anonymized information on the relative risk posed by all the Assessed Vulnerabilities. That anonymized information is sufficient to demonstrate that the risk being addressed by the TLSE Project – i.e., a winter T-South no flow event – is orders of magnitude greater than any of the other resiliency risks. It is beyond any reasonable question that FEI is targeting the right risks with the TLSE Project;
- Interveners and the public can also see the relative risk mitigation provided by different Supplemental Alternatives, and the analysis that was used to determine it; and
- Exponent has provided a detailed explanation of its analysis using anonymized information. The methodology is public.

[4] Exhibit C1-23, p. 1.
[5] See e.g., Exhibit B-61-1, Appendices RP4-05, RP4-20 and RP4-52 (pp. 1-2 of each).
[6] See Rule 6.3: https://www.ordersdecisions.bcuc.com/bcuc/orders/en/234282/1/document.do.
[7] Exhibit C2-17, p. 2.

Interveners do not need to see, for instance, the specific locations, physical features and risk factors of Assessed Vulnerabilities, especially those that are not addressed by the TLSE Project. It took FEI and Exponent over a year to complete and compile the physical engineering analysis of the infrastructure, such that interveners would not be able to replicate it in any event. Interveners and the public have access to the information that would be necessary for them to test Exponent's methodology and calculations.

Fourth, FEI's request to limit access to the Restricted Confidential Information to the BCUC is not driven by the particular characteristics of interveners (e.g., intervention history, potential for improper use), as suggested by RCIA, but rather, the fundamental principle that limiting circulation provides the best security protection. The risk of this information being disclosed warrants implementing the best defense available, recognizing that FEI has made the vast majority of the 2024 Resiliency Plan publicly available for interveners to probe and test as part of this proceeding. This approach strikes a reasonable and appropriate balance.

Fifth, Section 5 of the public version of the 2024 Resiliency Plan discusses the risk of cyberattack on critical energy assets which should be carefully considered before the BCUC determines this issue. The Government of Canada's Canadian Centre for Cyber Security (Centre) recently released a report (June 2023) on The Cyber Threat to Canada's Oil and Gas Sector.[8] The introduction stated (p. 2):

> It is difficult to overstate the importance of the oil and gas sector to national security because much of our critical infrastructure depends on oil and gas products to operate. At the same time, critical infrastructure, and especially the energy sector, is increasingly at risk from cyber threat activity. In the United States, for example, Colonial Pipeline garnered international attention in May 2021 when it was forced to shut down the operation of one of the largest gasoline, diesel, and jet fuel pipelines in the US, due to a ransomware incident. Although the pipeline was restarted a few days later, the disruption in the fuel supply resulted in shortages that caused the re-routing of flights, panic buying, and short-term price spikes. It was estimated that, at the time that the pipeline was restarted, the Eastern US was only a few days away from experiencing food and other shortages from the disruption of fuel to other sectors such as truck transportation. The Centre's analysis, discussed in this section, suggests that there is now a material and increasing risk from cyber threat activity towards critical gas infrastructure from a variety of malicious actors.

A challenge with making this information available to third parties is that it is highly unlikely any of the recipients have the same level of cyberthreat protection in place as FEI. Despite best intentions, they become a technological "weak link" for malicious actors. FEI submits that the geopolitical context today is, if anything, more fraught than when the Centre issued its report.

Ultimately, FEI submits that it is in the best interests of customers and the public generally for the Restricted Confidential Information to remain available to the BCUC only. The BCUC is well-equipped to examine the information. Should the BCUC deny FEI's request for confidentiality of all or some of this information, or broadens who has access to it, FEI requests that, pursuant to Rule 22 of the BCUC Rules, it be provided an opportunity to make submissions as to what should be done with the information, such as revising or withdrawing the information.

[8] https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector.

If further information is required, please contact the undersigned.

Sincerely,

FORTISBC ENERGY INC.

Original signed:

Sarah Walsh

cc (email only): Registered Interveners