July 14, 2017

Kirsten Walli
Board Secretary
Ontario Energy Board
2300 Yonge Street, Suite 2700
Toronto, Ontario M4P 1E4

Re: Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario – Board File No. EB-2016-0032

Dear Ms. Walli:

Attached please find Cornerstone Hydro Electric Concepts Association's (CHEC) comments with respect to the Board's invitation to comment on the OEB's Staff Report to the Board on a proposed Cybersecurity Framework. This submission addresses the several aspects outlined in the OEB Letter dated June 1, 2017 and follows the same format (Attachment A).

CHEC is an association of seventeen (17) local distribution companies (LDC's) that have been working collaboratively since 2000. The comments over the following pages express the views of the CHEC members.

We trust these comments and views are beneficial to the Board's initiative. CHEC looks forward to continuing to work with the Board in this matter.

Yours truly,

Kenneth B. Robertson

Kenneth B. Robertson CPA, CGA, MBA
Finance/Regulatory Analyst
43 King St. West, Suite 201
Brockville, ON K6V 3P7
krobertson@checenergy.ca
519-872-1100

ATTACHMENT A

Comments on the "Staff Report to the Board on a proposed Cybersecurity Framework and Supporting Tools for Distributors".

Response: On page 7 of the framework, it states:

> "*Smaller distributors do not have the capacity to apply a framework without support*".

In CHEC's opinion, this statement seems to be an unfair generalization. Although it might be applicable to some small utilities, it is possible that smaller utilities are quite capable at applying the framework without support from a third-party. Furthermore, this comment implies that larger utilities are capable of applying the framework without support, which may or may not be the case.

The final bullet-point on page 7 states:

> "*Distributors expressed concern about the level of effort and cost to address the risk*".

The comment regarding small utilities is probably the result of the cost to the address the risk. That is, small utilities can likely apply and implement the framework without third-party support, however, the one-time costs to become compliant initially could be significant and may be difficult to justify to rate-payers, intervenors, Board Staff, and other stakeholders. The use of a variance account for these one-time costs is recommended.

Regulatory Requirements and Reporting:

Response: CHEC has no issues with the proposed regulatory requirements and reporting expectations. Upon reviewing the initial excel checklists, it may be perceived as being onerous, but this is expected considering it's the initial implementation of the cybersecurity standard. The annual self-certification requirement appears to be relatively straightforward.

It is noted that one of the biggest changes in the regulatory requirements will be the documentation via policies and procedures of controls that are already undertaken by LDC staff or third parties. It is this documentation, and the updating of contracts with third party providers to ensure the additional reporting is provided, that will take the most time and have the biggest cost.

Additional Implementation tools and guidance required:

Response: As part of the implementation, OEB staff are recommending that industry provide an initial report within three months after the framework is issued to review its effectiveness. Considering this is the initial implementation of the cybersecurity standard, it might be difficult to adequately implement and assess the framework within this time period. A timeframe in the order of six months is suggested.

It is also difficult at this point to fully understand how long it will take to become fully compliant. The initial assessment should include a review of how long it will reasonably take for LDCs to become compliant and whether the proposed 12 months is sufficient.

Adequate guidance with respect to integration of privacy requirements:

Response: CHEC sees no issues with respect to the guidance provided on the integration of privacy requirements at this time.

Other aspects to be incorporated:

Response: CHEC does not see the need to incorporate any other aspects into the proposed framework at this time. Other aspects that need to be incorporated into the framework may become more evident as the framework evolves.

Additional Comments:

Response: Does the OEB anticipate approving a deferral and variance account to capture any incremental costs associated with the implementation of the cybersecurity requirements? The ability to track and recover these additional costs are consistent with past processes.

Response: CHEC members assume that cyber-security reporting and progress will not become a measure on the Scorecard. This information is highly confidential and should not be available for public review in the public domain. Can OEB Staff confirm this assumption is correct?

Response: CHEC members assume information included in DSP plans (page 12) concerning capital investment in managing cyber-security will be at a high-level or limited due to the sensitive nature of the subject being posted on public websites (i.e. OEB website and LDC website).

Response – CHEC members have assessed the Risk Profile Tool and have found that most members (~80%) identify with a “Medium” risk profile. From a cybersecurity risk perspective, this would imply that there is very little inherent difference (one size fits all approach) between Ontario utilities. Since this is not the intent of the risk profile tool, we recommend a calibration of the tool prior to the fall implementation so that it clearly

differentiates between LDCs based on expected risk profiles. CHEC would be happy to assist the OEB in the calibration.