October 15, 2018

Ms. Kirsten Walli
Board Secretary
Ontario Energy Board
2300 Yonge St., Suite 2700
Toronto, ON M4P 1E4

via RESS and Courier

Dear Ms. Walli:

Re: Proposed Cyber Security Readiness Report & Amendments to Electricity Reporting and Record Keeping Requirements (RRR)
BOARD FILE NO.: EB-2016-0032

1. INTRODUCTION

The Coalition of Large Distributors ("CLD") appreciates the opportunity to provide comments on the proposed cyber security readiness report ("Cyber Report") issued by the Ontario Energy Board ("OEB" or the "Board") on September 20, 2018. According to the OEB, the Cyber Report is intended to provide the OEB with information regarding a licensed transmitter's or licensed distributor's cyber security readiness, including its risk assessment and the status of implementation of control objectives relying on the *Ontario Cyber Security Framework* ("Framework"). The OEB is proposing to require transmitters and distributors to file the Cyber Report as part of annual reporting under the *Electricity Reporting and Record Keeping Requirements* ("RRRs").

The CLD consists of Alectra Utilities Corporation, Hydro One Networks Inc., Hydro Ottawa Limited, Toronto Hydro-Electric System Limited ("THESL"), and Veridian Connections Inc.

2. COMMENTS

In comments previously filed with the OEB on the draft Framework and the Transmission System Code and Distribution System Code amendments proposing to adopt the Framework, the CLD expressed support for an approach in which reporting would serve as the first step in Framework implementation. The CLD acknowledged that an effective reporting regime would grant the opportunity for cultivating an early, common understanding of the roles and responsibilities for various parties to fulfill under the Framework.

The CLD therefore understands and appreciates the OEB's objective to receive information regarding a transmitter's or distributor's (hereafter jointly referred to as "licensee" or "licensees")

cyber security readiness. However, the CLD respectfully submits that the Cyber Report would benefit from certain enhancements and clarifications aimed at providing flexibility in reporting, so as to ensure that a complete picture can be presented to the OEB. In the CLD's view, these modifications would improve the quality and precision of information and insights that would be yielded through the Cyber Report.

In particular, specific enhancements that the CLD believes would be appropriate and would help optimize the quality of information reported to the OEB include providing greater flexibility to licensees in reporting on the status of their implementation efforts and allowing for separate reporting on cyber security and privacy, where appropriate.

To this end, the CLD offers the suggestions for enhancements and requests for clarifications outlined below, with respect to the form of the Cyber Report:

(i) Part 2 – Request for Information

The CLD recommends changing the wording in Part 2, as follows (proposed changes are underlined):

> "Using the Ontario Cyber Security Framework (Framework), licensees <u>shall identify the control objectives that would apply to their organization in accordance with their Inherent Risk Profile</u>. <u>Licensees shall be expected to determine the control objectives that they plan to implement and how they will be achieved based upon their assessment of their organization's cyber security risk tolerance.</u> This information is to be provided by completing Part 3 and Part 4 of this form."

The CLD believes that the modified wording above emphasizes that a licensee's risk assessment and cyber security risk tolerance should factor significantly into any decisions made by the licensee relating to the implementation of applicable Framework controls. The modified wording more explicitly reinforces the expectation that licensees will have been provided with flexibility in terms of how they implement the control objectives set forth under the Framework, assuming that a licensee's risk assessment and established risk tolerance supports a given implementation approach.

(ii) Part 3 – Acknowledgement of Status

The CLD encourages the OEB to clarify how licensees should complete this section of the Cyber Report.

For example, a licensee's implementation plan or plans could reflect aspects of more than one of the three implementation plan approaches listed – some control objectives may be implemented, others may be partially implemented, while others may be part of a phased plan for which implementation is pending. In turn, it is unclear whether a licensee should check

multiple boxes with respect to the status of its implementation plan or plans. Similarly, it is unclear whether and/or how this section appropriately acknowledges that the implementation of specific control objectives will vary from one licensee to the next depending on the licensee's risk profile.

Further guidance from the OEB in this regard would enhance licensees' understanding of how to complete Part 3 of the Cyber Report, as well as their understanding of how this section will provide the OEB with meaningful and comparable information regarding the state of cyber security in the sector, in light of the varied implementation approaches which licensees are set to undertake.

(iii) Part 4 – Supporting Information – Cyber Security

The CLD respectfully recommends the following enhancements to this section of the Cyber Report:

(a) Separate Responses for Cyber Security & Privacy: Each question should allow for separate reporting on the status of implementation efforts related to cyber security and implementation efforts related to privacy. Options for effectuating this outcome could include splitting each question into two subparts or incorporating separate check boxes.

The CLD believes that such an approach is appropriate as it recognizes that, for some licensees, functions related to cyber security and privacy are separate, albeit complementary. Accordingly, the implementation of control objectives by these licensees for applicable areas of the Framework may occur in different ways and in different phases.

For example, for any given risk area that is covered under the scope of a question in Part 4, it is possible that a licensee may be taking (or have taken) action to implement control objectives related to cyber security, but may be at a different phase of action in relation to privacy. A response of "Not Implemented" in this instance would not provide an accurate reflection of the status of control objective implementation for this licensee.

Similarly, the CLD observes that privacy is referenced in Questions 9-12 pertaining to the Respond and Recover functions. However, the 11 privacy controls outlined in the Framework only correspond to the first three functions set forth in the Framework – i.e. Identify, Protect, and Detect.

(b) Comment Box to Enable More Flexibility in Responding: The CLD strongly requests that the Cyber Report grant licensees the flexibility to provide comments and/or explanations regarding the status of their control objective implementation. As an initial matter, there are important details and nuances regarding a licensee's implementation status which cannot be effectively or clearly communicated through any response to the proposed

questions. What's more, the inclusion of a comment box would be consistent with the approach taken for several existing RRRs. Likewise, this approach would mitigate or obviate the need for the OEB to circle back with a licensee to seek additional information on the basis for that licensee's answers to a question or questions.

(c) Additional Response Options: In addition to "Implemented" and "Not Implemented", the CLD believes that licensees should have other options for responding. Possible examples include "*Partially Implemented*" and "*Plan is in place for implementation*", or alternatively, *"In Progress."* Likewise, there is a need for a *"Not Applicable"* option.

The inclusion of these options would account for the prospect that a licensee may be at any one of these possible phases in its implementation activity, depending on its risk profile and implementation plan. In turn, the inclusion of these response options would provide the OEB with more meaningful information regarding a licensee's implementation plan and cyber security maturity level.

(d) References to Specific Control Objectives or Framework Categories/Subcategories: The CLD observes that, in one instance, the proposed Cyber Report offers a specific point of reference to help illustrate the intended scope of a specific question. Question 1 includes a footnote which clarifies the Cyber Report's understanding of the term "governance."

While this is the only question in Part 4 that includes a supplementary reference, it may be helpful to replicate this approach for other questions. If there are particular control objectives and/or Framework subcategories that are top of mind for the OEB in regard to specific questions, then cross-referencing these items can help ensure that a licensee is correctly interpreting the intended scope of the question.

For example, Question 5 refers to "mitigation plans" in the context of the Protect function under the Framework. However, in the Framework itself, mitigation controls are referenced in the descriptions of the Initial Achievement Levels associated with particular categories and subcategories under the Protect function, but not in others. If there are specific control objectives which the OEB believes should be covered under such mitigation plans, then the CLD requests that the Cyber Report offer guidance or reference points to that effect.

In addition, with regards to Question 4, the CLD suggests that it may not be appropriate to ultimately include this question in the final Cyber Report. As noted on page 2, the Cyber Report is intended to serve as a status report for the period January 1, 2018 to December 31, 2018. At the time of filing, however, the Independent Electricity System Operator ("IESO") has not yet implemented the July 2018 amendment to its license, which requires the IESO to make information sharing services available to licensees. While the IESO may be able to begin

rolling-out information sharing services in late 2018, it is nevertheless unlikely that licensees will be able to cultivate significant experience in using these services prior to the end of 2018.

(iv) Other/Miscellaneous

- Intended Use of Licensee Reporting: The CLD requests additional detail and guidance on how the OEB intends to act upon the information that is gathered from licensees by way of the Cyber Report and accompanying RRRs. Based upon the scope of questions that are set forth in the proposed Cyber Report, it remains unclear to CLD members how exactly licensees' responses will be evaluated by the OEB and translated into an assessment of the sector's overall cyber security readiness.

  Moreover, the OEB's letter proposes that licensees will be required to submit a completed Cyber Report annually, as part of RRR reporting. At the same time, however, the purpose of the Cyber Report is stated to be enabling the development of a baseline of the sector's readiness. It is therefore unclear to the CLD whether the OEB intends the form of the Cyber Report to remain constant for annual reporting purposes into the foreseeable future, or whether the OEB intends to modify the form of the Cyber Report each year with the aim of updating its original baseline assessment.

- Utilization of Common Cyber Report by Affiliated Licensees: The CLD believes that all aspects of Framework implementation, including annual reporting, should recognize and allow for the prospect of a large licensee's cyber security infrastructure and/or privacy program applying to more than one licensed entity within its corporate family. Accordingly, the Cyber Report should enable a licensed entity (Licensee A) to reference an affiliated licensed entity's (Licensee B) Cyber Report where there is dependence on, or shared use of, the same systems and programs by both licensees.

3. CONCLUSION

The CLD appreciates the opportunity to provide comments on the proposed Cyber Report and respectfully requests that any subsequent action taken by OEB be consistent with the comments set forth herein.

If you have any questions with respect to the above, please contact the undersigned.

Sincerely,

Original signed by Indy J. Butany-DeSouza

Indy J. Butany-DeSouza, MBA
Vice President, Regulatory Affairs
Alectra Utilities Corporation

Indy J. Butany-DeSouza
Alectra Utilities Corporation
(905) 821-5727
indy.butany@alectrautilities.com

Andrew Sasso
Toronto Hydro-Electric System Limited
(416) 542-7834
asasso@torontohydro.com

Gregory Van Dusen
Hydro Ottawa Limited
(613) 738-5499 x7472
GregoryVanDusen@hydroottawa.com

George Armstrong
Veridian Connections Inc.
(905) 427-9870 x2202
garmstrong@veridian.on.ca

Jeffrey Smith
Hydro One Networks Inc.
(416) 345-5721
jeffrey.smith@HydroOne.com