January 18, 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: Notice of Proposal to Amend a Code, *Proposed Amendments to the Transmission System Code and the Distribution System Code to address Cyber Security for Electricity Transmitters and Distributors*
BOARD FILE NO.: EB-2016-0032

On December 20, 2017, the Ontario Energy Board ("OEB" or the "Board") published a Notice of Proposal to Amend a Code, *Proposed Amendments to the Transmission System Code and the Distribution System Code to Address Cyber Security for Electricity Transmitters and Distributors*.

The purpose of the proposed Transmission System Code ("TSC") and Distribution System Code ("DSC") amendments is to establish regulatory requirements for all licensed transmitters and distributors and to provide the OEB with information to demonstrate that regulated entities are taking appropriate actions relative to potential cyber security risks. The amendments rely on the establishment and use of the industry-developed Ontario Cyber Security Framework ("the Framework"), as the common basis for assessing and reporting cyber security capability to the OEB. The proposed amendments would add definitions for Cyber Security and the Framework to the TSC and DSC; establish regulatory reporting requirements for all licensed transmitters and distributors to report their cyber security maturity based on their assessment against the Framework, and to provide the necessary information and self-certification on an annual basis; and define the continuing obligations regarding the reliability and integrity of the transmission and distribution system and protection of personal information.

The Coalition of Large Distributors ("CLD") and Hydro One Networks Inc. are pleased to offer comments on these proposed amendments. The CLD consists of Alectra Utilities Corporation, Hydro Ottawa Limited, Toronto Hydro-Electric System Limited ("THESL"), and Veridian Connections Inc.

A. SUMMARY OF KEY MESSAGES & RECOMMENDATIONS

1. The CLD supports the extensive consultation work undertaken by the OEB in the interest of developing an industry-wide standard for cyber security.

2. The CLD supports the OEB's view that the ongoing implementation of the Cyber Security Framework is best developed and led by the industry through collaboration and information sharing. The CLD remains supportive of the concept of a Cyber Security Advisory Committee ("CSAC") and seeks clarification from the OEB that formation of the CSAC is still planned.

3. The CLD supports the proposed regulatory reporting requirements as appropriate and worthwhile first steps towards implementing the Framework.

4. The CLD supports the addition of specific language in the TSC and DSC in order to reflect the industry's focus on robust cyber security principles. However, the CLD would like the inclusion of physical security in the definition of Cyber Security to be modified.

5. The CLD believes that maintaining a strong focus on cost-effectiveness and value for ratepayers will be a critical success factor in implementation of the Framework, similar to any other planned regulatory action or initiative.

6. The CLD observes that uncertainty persists regarding aspects of Stage 2 implementation, but nevertheless appreciates the specific signals from OEB that a measured, industry-led approach to implementation of Stage 2 objectives of the Framework is planned. Specifically, the CLD does not believe Stage 2 of the Framework should specify audit requirements until there is sufficient information and experience gained to justify this need.

B. BACKGROUND

Consultation Overview

By letter dated February 11, 2016, the OEB initiated a policy consultation to review cyber security practices of the (non-bulk) electricity grid, as well as the natural gas system. Given the lack of an acceptable standard across the system, the OEB undertook discussions with licensed distributors and transmitters, as well as other stakeholders, to develop an industry framework for the assessment of the actions these entities take to address cyber security. To achieve this, the OEB established a Cyber Security Working Group ("CSWG") comprised of distributors, transmitters and other stakeholders, in addition to an expert consulting team to support this work. The CSWG and expert consultants developed an initial Cyber Security Framework, which was detailed in the white paper entitled *Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets.*

This white paper was released in June 2017 alongside a *Staff Report to the Board* on a *Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors* that set out Board Staff's view on cyber security, and OEB expectations on the proposed Framework, including the benefits of the approach developed by the CSWG. Comments were due on July 15, 2017. The CLD submitted comments on the OEB Staff Report and proposed Framework.

Notice of Proposal Summary

The Notice of Proposal outlines the proposed changes to the TSC and DSC as they relate to cyber security. These include the addition of the definitions of Cyber Security and the Framework, which will capture the key concepts related to the implementation of the cyber security policy.

The OEB is proposing to amend the TSC and DSC to require that licensed distributors and transmitters report their cyber security status based on their assessment against the Framework, and provide the necessary information and certification to the OEB on an annual basis. This assessment will be reported through a self-certification report signed by the Chief Executive Officer of the licensee.

Specific details of the reporting requirements will be established in the OEB's *Reporting and Record Keeping Requirements* ("RRR"). The OEB will work with licensed transmitters and distributors to develop the certification requirements.

The OEB proposes that an initial report is submitted three months after these Code amendments come into force. Subsequent reporting will be completed on an annual basis. It will align with the existing RRR filings and is expected to begin in 2019.

At this time, the OEB is soliciting comments on the proposed amendments to the TSC and DSC.

C. COMMENTS – GENERAL

i. Support for Consultation Process

CLD members recognize the robust stakeholder engagement undertaken by the OEB through both the Cyber Security Steering Committee ("CSSC") and CSWG, in soliciting input and helping to develop the Framework. These groups have incorporated the feedback provided by the broader stakeholder community into changes made to the Framework as well as the proposed implementation plan for the Framework.

As the Framework evolves based on technological advances, continuous improvement, and the recognition of best practices, it will be critically important to preserve and enhance the collaborative environment that has been established.

ii. Scope of the Framework

The original proposal from June 2017 signaled plans to extend the Framework to unit sub-meter providers, retailers, and marketers. The status of this intended action is not clear, as neither the Notice of Proposal nor the updated Framework address this matter. The CLD requests that clarification be provided on the applicability of the Framework to other entities in the industry, beyond licensed distributors and transmitters.

D. COMMENTS – SPECIFIC

Proposed New TSC and DSC Amendments

i. Definitions (section 1.2)

The CLD supports the inclusion of the definitions of "Cyber Security" and "Cyber Security Framework" into both the TSC and DSC. The Framework will benefit both distributors and consumers by offering minimum standards to which all distributors must comply. Accordingly, it is worthwhile having these principles entrenched in the Codes.

However, the proposed definition of cyber security is worded such that both electronic and physical security are included. Physical security encompasses a broad range of issues, not all of which are directly linked to cyber security. The CLD proposes modifying the definition to narrow the scope to physical security issues as they relate to cyber security protection.

ii. Regulatory Requirements and Reporting (section 6.8.1)

The CLD remains supportive of the proposed regulatory reporting requirements, and views them as appropriate and worthwhile first steps towards implementing the Framework. The CLD believes that the establishment and implementation of an effective reporting regime represents a sound point of departure in this broader effort. This initial movement forward will grant the opportunity for cultivating an early, common understanding of the roles and responsibilities for the various parties to fulfill under the Framework.

The CLD observes that the reporting options included in the self-certification process are limited to "compliant" and "non-compliant". However, not all aspects of the Framework are universally applicable to all utilities, and the self-certification document should reflect a utility's ability to self-identify as being compliant even if they have not implemented a component of the Framework that they have determined is not applicable or not relevant. The CLD proposes modifying the wording in the self-certification document to recognize that not every component of the Framework may be applicable to all utilities.

The OEB has stipulated that details of the reporting requirements will be established in the OEB's RRR and that work will be conducted in partnership with licensed transmitters and distributors to develop the certification requirements. The CLD appreciates the OEB's collaborative approach in this regard and looks forward to participating.

In its July 2017 comments, the CLD requested additional details on whether and how the OEB intends to disclose the certification status of distributors and other regulated utilities. The CLD was pleased that in this Notice of Proposal, the OEB acknowledged the sensitive nature of the reports and indicated that they will be filed in confidence and segregated from other Board records.

Notice of Proposal & Framework – Other Items

iii. Cost and Resources

The CLD recognizes that implementation of the Framework and cyber security practices in general will come at a cost to distributors, on both a financial and resource allocation basis. Protecting utility operations and customer information from cyber-attacks will require an ongoing commitment to continuously improve security protocols, and to leverage best practices learned from others in the industry. Accordingly, the CLD appreciates the OEB's acknowledgment in its Notice of Proposal that transmitters and distributors will be incorporating additional cyber investments into their system plans

The CLD wishes to reinforce its prior observation that maintaining a strong focus on cost-effectiveness will be a critical success factor in the implementation of the Framework. With a range of new requirements, entities, and implementation support resources contemplated under the Framework, it will be imperative for all parties to ensure that value for ratepayers remains an enduring principle and objective in the execution of this effort.

iv. Implementation of Stage 2 Requirements of the Framework

In its July 2017 submission, the CLD expressed concern that the OEB Staff Report and the proposed Framework left many essential implementation and compliance-related details uncertain – especially in relation to requirements and actions contemplated under Stage 2. Respectfully, the CLD observes that, while the OEB has made certain updates to the Framework and provided guidance in terms of its approach to implementing the Framework, uncertainty persists regarding several aspects of Stage 2. These include:

- Do all distributors need to fulfill Stage 1 requirements before any transition to Stage 2?
- How will Central Compliance Authority ("CCA") structures and processes be governed and funded?
- What is the governance structure of the CCA and when will it be established?

- How will the role and functions of the CCA evolve (i.e. transition from Stage 1 to Stage 2) as identified on page 16 of the Framework document?
- How will the evolution of the CCA correlate with the cyber security maturity levels of distributors?

The CLD firmly believes that the industry should play a prominent part in establishing the role and functions of the CCA and that subsequent industry collaboration should address such issues and uncertainties. As the state of cyber security readiness begins to improve within the sector, the CLD continues to caution against an approach to cyber security that would become overly or solely reliant on auditing activities for assessing compliance. It is the CLD's view that establishing audit requirements in Stage 2 of the Framework, at this stage in its development, is premature. The inclusion of audit requirements in Stage 2 should be considered after the OEB has had more experience with the implementation of the Framework, and information has been collected to justify the need for such requirements as part of the Framework's evolution. Therefore, the CLD requests that specific requirements related to auditing activities be removed from Stage 2 of the Framework.

The Notice of Proposal recognizes that much more work is required around the requirements and actions which are set to serve as the basis for Stage 2 as the maturity levels of cyber security controls and protections within the sector improves. In addition, it conveys an expectation that industry will: (a) work collaboratively to evolve the Framework and address Stage 2 components "when and if it is felt that it will enhance licensees' ability to meet their obligations"[1] and (b) have appropriate flexibility to make cyber security decisions that are determined by their assessment of risk in meeting compliance obligations. The CLD supports the OEB's decision to focus the scope of these initial proposed Code amendments on interim reporting and annual self-certification.

v. Cyber Security Advisory Committee ("CSAC")

In its July 2017 comments, the CLD had expressed support for the proposed formation of the CSAC and for this body serving as the central forum for dialogue on future implementation and compliance activity. The CLD continues to share the OEB's view that it is incumbent upon the industry to take ownership of the Framework and its evolution, and that a dedicated forum comprised of industry and stakeholder experts is the most effective means for doing so.

The CLD had anticipated that the OEB's Notice of Proposal would re-affirm the concept and the role of the CSAC, as articulated in the original OEB Staff Report. However, the Notice of Proposal makes no explicit reference to the CSAC. Instead, the Notice of Proposal indicates that the CSWG will remain in place until other industry forums and associations are able to assume responsibility for evolving the Framework.

[1] Notice of Proposal, p. 9.

The CLD seeks clarification from the OEB that the CSAC is still intended to be chief amongst these groups.

vi. Cyber Security Information Sharing Forum

Whereas the OEB Staff Report had proposed mandating all distributors to participate in an information sharing forum, the Notice of Proposal signals an expectation of the industry to collaborate with the Independent Electricity System Operator ("IESO") on developing and institutionalizing an approach to information sharing in which a central agency provides this service to all industry participants.

The CLD supports the Notice of Proposal's suggested approach to collaborate with the IESO on this important initiative.

E. CONCLUSION

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

The CLD remains committed to collaborating with the OEB and all stakeholders, especially in relation to providing assurances that utilities are taking appropriate action to address cyber security risks and to fulfill privacy obligations.

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

Ed Machaj
Hydro One Networks Inc.
(416) 345-5090
ed.machaj@hydroone.com