July 15, 2017

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: Staff Report to the Board on a Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors;
Board File No. EB-2016-0032

On June 1, 2017, the Ontario Energy Board ("OEB" or the "Board") issued its *Staff Report to the Board on a proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors* (the "Staff Report"), and the accompanying industry developed *Cyber Security Framework* (the "Framework"). The Staff Report and proposed Framework are being issued for comment.

The Coalition of Large Distributors ("CLD") and Hydro One Networks Inc. are pleased to offer comments on these proposals. 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 submits that its comments within this submission are intended to help utilities implement stronger cyber security controls and thus provide a stronger security posture to protect customers.

2. The CLD supports the proposal to anchor the Framework in the NIST Framework. CLD members have implemented the NIST Framework within their respective organizations and lead the sector in Ontario, in this regard.

3. The CLD is concerned that the Framework too quickly relies on auditing and compliance to regulate cyber security in this initial roll-out stage.

4. Framework implementation should take the form of an iterative and collaborative approach, and build on collaboration that has been cultivated through this consultation.

5. The CLD supports the proposals for interim reporting and self-certification as appropriate and worthwhile first steps towards implementing the Framework.

6. OEB Staff's Report leaves many essential implementation- and compliance-related details uncertain.

7. The CLD recommends that OEB temporarily refrain from seeking to finalize details related to post-Stage 1 implementation and compliance, and that parties be granted the opportunity to cultivate experience with interim reporting and self-certification processes.

8. The CLD recommends that subsequent dialogue on the future stages of implementation and compliance occur within the proposed Cyber Security Advisory Committee.

9. Cost-effectiveness, as well as cost recovery measures, must be taken into account as part of the Framework's implementation, similar to any other planned regulatory action or initiative.

10. The CLD remains fully committed to the protection and privacy of customer information. However, the CLD respectfully submits that several aspects of how privacy principles are intended to be fully incorporated into the Framework remain unclear. This requires further investigation and consideration.

11. With respect to the proposed Cyber Security Information Sharing Forum, efficiencies and synergies can be achieved by leveraging existing forums which may be able to achieve the OEB's proposed objectives (e.g. IESO Cyber Security Forum).

12. The CLD supports the proposed formation of the CSAC and believes that CSAC should serve as the central forum for dialogue on future implementation and compliance activity.

B. BACKGROUND

Consultation Overview

By letter dated February 11, 2016, the OEB initiated a consultation to review the cyber security of the non-bulk electrical grid and associated business systems in Ontario that could impact grid reliability and the protection of personal information.

The consultation was designed to establish a cyber-security policy and reporting requirement that provides the OEB with the assurance of distributor cyber security capability. In the absence of an existing distribution cyber security standard, the primary focus of the first phase of the consultation was on distributors' requirements leveraging recognised industry standards, policy guidelines and auditing requirements. The Board also initiated a communication strategy to reach out to various stakeholder groups throughout the policy development process and ensure adequate sector representation and input in the consultative process. The OEB retained consultants that were commissioned to work with the Cyber Security Working Group ("CSWG") to develop and document the process and tools to manage cyber security in a manner consistent with the objectives set out by the OEB.

Report Overview

The Report provides a background on the OEB's expectations in relation to cyber security and privacy in the energy sector. These expectations, as identified by OEB staff, include the protection of the privacy of consumer information, the protection of network systems and operations from risks related to cyber-attacks, and appropriate consideration in distributors' system plans of cyber security risks, based on industry best practices.

The Report proposes policy and reporting requirements to provide measurable assurance to the OEB that Ontario's electricity distributors address cyber security risks based on a consistent approach and set of criteria in order to meet their reliability, security and privacy obligations.

The Report also suggests that the proposed Framework should apply to electricity transmitters and natural gas distributors, in order to provide similar assurance to the OEB.

The Framework is expected to be in place by late 2017. OEB staff is proposing interim reporting by LDCs on cyber security assessment and progress within three months of the Framework being issued, as well as an annual certification of cyber security capability starting in 2018.

OEB staff is proposing that the Framework be supported by new industry working groups to facilitate the continuous improvement of the Framework through ongoing sector consultation with a broad spectrum of third party stakeholders and regulated entities.

At this time, the OEB is soliciting comment on both the Report and the Framework. In particular, OEB is specifically interested in stakeholder feedback regarding the following:

- Regulatory Requirements and Reporting;
- Additional Implementation tools and guidance required;
- Adequate guidance with respect to integration of privacy requirements; and
- Other aspects to be incorporated.

C. COMMENTS – GENERAL

i. Support for NIST

The CLD supports the proposal to anchor the OEB's framework in the U.S. National Institute of Standards and Technology ("NIST") Framework. CLD views the NIST Framework as being consistent with the OEB's Renewed Regulatory Framework ("RRF"), insofar as it is principles-based and outcomes-focused. CLD members have adopted the NIST Framework as a core element of their cyber security risk management and mitigation activities. The CLD believes that working from the NIST Framework, which is used extensively in other jurisdictions, is favourable to a made-in-Ontario approach. Adoption and implementation of the NIST Framework will help ensure a consistent approach to addressing cyber security risks amongst all Ontario utilities, regardless of size and current security posture.

ii. Support for the Consultation Process

CLD members appreciated the OEB's extensive engagement with stakeholders through both the Cyber Security Steering Committee ("CSSC") and Cyber Security Working Group, in soliciting input and helping to develop the Framework. We see significant value in engaging subject matter experts ("SMEs") as part of a policy consultation process. The Framework is consistent with much of the strategic direction of the CSSC and incorporates practical tools and mechanisms to support the understanding and implementation of the Framework, as identified by the CSWG.

The CLD draws encouragement from the collaboration and openness that served as a hallmark of the CSSC and CSWG efforts. Moving forward into the next phases of this initiative, the CLD urges the OEB and all stakeholders to preserve and expand the collaborative environment that has been established. In light of our comments in this submission, we believe the process could be further improved if regulatory experts are included with SMEs as part of the working group process going forward, to ensure a full debate can be held prior to formal written comments being solicited.

iii. Ensuring an Appropriate Pacing of Next Steps

Given the highly dynamic and constantly shifting threats that pose a risk to cybersecurity, the CLD believes that the primary focus of the OEB's regulatory framework should be continuous improvement within Ontario's electricity sector, underpinned by a culture of collaboration that fosters information sharing and best practice deployment. Implementation of the Framework represents a unique opportunity to achieve a baseline level of alignment and consistency within the sector, and in turn, to obtain valuable assistance in the movement towards increasingly robust and mature cyber security protections.

The CLD is of the view that a key determinant of success in this context will be subscribing to a "walk before you run" approach. The Report and Framework appropriately acknowledge that the cyber security risk landscape is in a constant state of change, and that there are a range of cyber risk profiles and maturity levels across utilities in Ontario. Accordingly, in the CLD's view, it is imperative that implementation take the form of a truly iterative and collaborative approach, so that utilities have the opportunity to incorporate solutions and best practices in an environment that emphasizes improvement, maturation and outcomes. What's more, movement at a measured pace through subsequent phases of implementation and learning will ensure the cultivation of a shared understanding of the appropriate roles and responsibilities for all affected parties to fulfill.

iv. Cyber as One Link in a Utility's Overall Security Chain

Finally, the CLD observes that while it is entirely appropriate for the OEB to focus policy efforts on cyber security, that it not overshadow the critical interrelationship it plays with the physical security of the utility. Strong physical security can complement strong cyber security by, for example, making access to cyber networks more difficult. We encourage the OEB to give consideration to this relationship through the standard rate application process.

D. COMMENTS – SPECIFIC

Guided by the general principles and perspectives outlined in the section above, the CLD offers the following comments on specific elements of the Framework.

Notwithstanding the CLD's strong support for utilization of the NIST Framework, CLD members have a number of questions and concerns in regards to several aspects of the OEB Staff's proposals. In particular, **the CLD is concerned that the Framework's emphasis is auditing and compliance**. Whereas audit and compliance frameworks may be appropriate regulatory mechanisms for other established and mature utility processes or practices, the CLD would caution that such an approach may be ineffective (or perhaps counterproductive) in the unique context of evolving cyber security risks.

In the comments below, the CLD elaborates further on these and other issues.

i. Regulatory Requirements and Reporting

The OEB is proposing that the Framework be in place by late 2017, followed by interim reporting within three months, and with annual reporting starting in 2018. While the timeline for initial regulatory action appears relatively straightforward, the CLD is very concerned that OEB Staff's Report leaves many essential implementation- and compliance-related details uncertain. Upon review the Report and Framework, it remains unclear what the answers are to fundamental questions such as the following:

- Will an LDC be required to prepare a compliance plan, in support of its annual self-certification?[1]
- What is the intended timeline for moving from Stage 1 to Stage 2 implementation? Will all LDCs be required to complete Stage 1 before the transition to Stage 2 occurs?
- Is OEB proposing to adopt, either in whole or in part, the components of Stage 2 implementation, as outlined in White Paper? (e.g. establishment of a Centralized Compliance Authority);
- What entity(s) will audit LDCs and evaluate their security controls? What form of accreditation will third-party organizations undergo? Could LDCs certify these organizations, in order to ensure that auditors possess expert knowledge of the Framework and, in turn, ensure consistency among the audits performed? When should LDCs expect these independent audits to occur?
- Who will ultimately be responsible for developing Key Risk Indicators?
- What safeguards and controls will be adopted to ensure the protection and confidentiality of sector participants' sensitive information?
- What uses are contemplated by the OEB for the information and data that it will receive from utilities? How does the OEB intend to use this data for purposes of assisting utilities in their journey towards greater maturation of cyber security controls and protections?

In light of the number (and the nature) of questions raised by the Framework's proposals for implementation and compliance, the CLD respectfully submits that specific aspects of these proposals should be revisited and refined. In particular, **the CLD has significant concerns regarding what is proposed for Stage 2 implementation, as well as the lack of clarity and certainty engendered by the incongruence between the OEB Staff Report's proposals for Stage 2** and those that are set forth in the Framework itself. The CLD is not confident that

[1] Page 29 of the Report hints at a proposed requirement for a compliance plan. However, this language is not echoed elsewhere in the Report or the Framework.

effective implementation and compliance under Stage 2 can be achieved, based on the current (and conflicting) descriptions of Stage 2 in the two documents.

Moreover, the CLD respectfully observes that an underlying premise of the Framework appears to be that the exact details of the configuration and timing of future activity must be firmly carved out and enshrined at this particular point in time. However, the CLD urges the adoption of an alternative philosophy and approach in this regard.

With respect to examining the potential design and set of timelines for post-Stage 1 implementation, the CLD believes that the interests of all parties will be best served if restraint is exercised at this stage of the process. In step with the general comments articulated by the CLD above, the CLD is of the view that the continuously evolving risk landscape, coupled with the relative uniqueness and novelty of the regulatory framework that is being contemplated, should behoove the OEB and stakeholders to move forward at a measured pace. Likewise, the journey towards continuous improvement in cyber security should be undertaken in a manner that allows for early experience to be accumulated and internalized effectively, with ample space and time for the incorporation of lessons, insights, and best practices, and for the sharing of information in support of such outcomes.

Accordingly, the CLD believes that an appropriate first step is to focus collective resources and attention on establishing, and gaining familiarity with, a robust framework foundation that will serve as a strong, stable, and secure springboard for future action.

To this end, **the CLD recommends that OEB temporarily refrain from seeking to finalize the details relating to post-Stage 1 implementation and compliance**, and that all parties be granted the opportunity to cultivate early, fulsome experience with the interim reporting and self-certification processes.

And looking ahead, the CLD is of the view that the proposed Cyber Security Advisory Committee ("CSAC") is an optimal forum for subsequent dialogue between OEB and stakeholders on what future stages of implementation and compliance should look like.

The CLD offers these recommendations in the spirit of helping to ensure that all parties take the time necessary to ensure that short-, mid-, and long-term implementation and compliance requirements are appropriately evaluated, thoroughly understood, and clearly communicated. These recommendations reflect what the CLD views as legitimate concerns surrounding (i) how future stages of implementation and compliance have been described in the Report and Framework, and (ii) whether stakeholders' interests are best served at this time through the prescription of future requirements. At the same time, the course of action recommended herein can begin providing the OEB with assurances that utilities are taking meaningful steps to assess and manage cyber security risks, and to protect customer information.

Given the multitude of unique, sensitive, and unfamiliar factors at play in this initiative, the CLD views the aforementioned recommendations as reasonable and valuable next steps, and ones which will position all parties for a successful beginning to the journey towards continuous improvement and maturation.

Annual Certification

Consistent with the above discussion on regulatory requirements, **the CLD views the proposals for interim reporting and self-certification as appropriate and worthwhile** first steps in implementation of the Framework.

Nevertheless, the CLD requests the OEB to provide further detail on the process that will ensure if an LDC is unable to certify full compliance. Likewise, the CLD requests additional details on whether and how the OEB intends to disclose the certification status of LDCs and other regulated utilities.

The establishment of industry-wide accountabilities is a key component of this Framework. Such accountability will help ensure that deficiencies are addressed in a timely and effective manner. In view of the interdependent nature of cyber security risk mitigation in the sector, it would benefit all parties to have line of sight into potential weaknesses or exposures.

Implementation & Compliance Costs

The CLD observes that both the Report and Framework are largely silent on the cost implications and considerations associated with their respective proposals. While not seeking to minimize the critical importance of investments in cyber security protections, the CLD believes that costs and cost-effectiveness must be taken into account as part of the Framework's implementation, similar to any other planned regulatory action or initiative. This comment is especially germane in the context of the potential for new entities to be stood-up under the Framework (e.g. Centralized Compliance Authority). In the absence of cost-effectiveness considerations, there is a further element of risk as LDCs strive to achieve an acceptable balance between rate and business impacts.

Moreover, to the extent that the proposed regulatory framework will impose more stringent requirements (and thus costs) upon larger LDCs than all LDCs on average, we are concerned that this will impact the conclusions that can be drawn from the OEB's total cost benchmarking framework that establishes stretch factors for the purposes of ratemaking.

Linkages to OEB Consultation on Corporate Governance Guidance

In light of the regulatory and reporting requirements that are proposed, this Framework would obviate the need for LDCs to report on cyber security incidents and risk management to the OEB, as proposed under the separate OEB consultation on Corporate Governance Guidance for OEB Rate-Regulated Utilities.[2] The CLD views this as a reasonable approach that would eliminate the prospects of duplication and inefficiencies. CLD requests clarity on this matter in the final version of the Framework.

ii. Additional Implementation Tools and Guidance Required

As a general matter, the CLD agrees that the provision of guidance will be essential to successful implementation of the Framework over the long-term by the sector. The CLD believes that, first and foremost, OEB and stakeholders should seek to maximize the use of

[2] EB-2014-0255.

existing guidance, especially that which is specific to the electricity and natural gas sectors. There are many existing resources that should be examined and adopted, and assessed for possible enhancements or customization, within the Ontario context.[3] Such an approach will support efficiency and cost-effectiveness in the provision and application of guidance, by building upon existing resources and best practices.

On the specific matter of periodic assessments of an entity's level of risk, the CLD observes that the Report makes reference to the permissibility of both subjective and objective approaches.[4] The CLD seeks clarity regarding the degree of latitude that LDCs will have to determine a risk profile that aligns with their specific operational needs and exposures. Some form of guidance may be required to help standardize these periodic risk assessments, in order to mitigate the risk of not having comparable baselines across utilities. In addition, further clarification on the intent of the subjective approach would be helpful.

Benchmarking and Metrics

The Report includes numerous references to benchmark objectives and controls, as well as the potential for benchmarking of cyber security capabilities.[5] As a general principle, the CLD agrees that consistency and comparability will aid utilities in assessing their security controls and risk mitigation, and in sustaining their movement along the path of continuous improvement.

The CLD suggests that early experience with Framework implementation will provide valuable lessons and insights, with respect to what entity(s) are best-suited to the performance of benchmarking activity and the preparation of metrics. The CLD supports further discussion on this issue and opportunity within the CSAC.

iii. Adequate Guidance with Respect to Integration of Privacy Requirements

As a general principle, **the CLD wishes to stress that its members remain fully committed to the protection and privacy of customer information.** CLD members take seriously their obligations to serve as responsible stewards and custodians of customer information, and to safeguard such information against inappropriate disclosure.

At the same time, the CLD respectfully submits that several aspects of how privacy principles are intended to be fully incorporated into the Framework remain unclear. In particular, there does not appear to be any discussion of potential implications or uncertainties associated with certain Privacy by Design principles – especially against a backdrop of heightened public policy interest in maximizing data access and value.

The CLD suggests that this is another issue that is ripe for further discussion within the CSAC.

iv. Other Aspects to be Incorporated

Cyber Security Information Sharing Forum (CSIF)

[3] For example, the U.S. Department of Energy prepared "Energy Sector Cybersecurity Framework Implementation Guidance" in September 2014 as a sector-specific tool for NIST Framework implementation.
[4] Report, p. 25.
[5] Report, pp. iv, v, 6, and 19.

Assuming the OEB chooses to proceed with the decision to make participation in the new CSIF mandatory for all utilities, the CLD believes that efficiencies and synergies can be achieved by the OEB and stakeholders seeking to leverage existing forums which may be able to achieve the OEB's proposed objectives. For example, the IESO administers a Cyber Security Forum, with which many industry participants (of all sizes) already have a high degree of familiarity and confidence in the value derived from the collaboration that the IESO has been able to facilitate. As the OEB is well aware, the IESO plays a unique, value-added convening role in the context of many other stakeholder engagements on policy and operational issues, as well as in the context of larger grid security simulations such as the North American Electric Reliability Corporation's ("NERC") biennial GridEx exercises.

In addition, there are a few aspects of the OEB's proposal for which the CLD is seeking greater clarity. First, it is unclear to the CLD how the OEB intends to enforce mandatory CSIF participation by sector participants. In addition, the CLD is unsure whether the OEB intends the CSIF to be an in-person forum or a virtual platform. In either case, the confidentiality and protection of information that is shared within the CSIF must be a top priority. Additional information from the OEB is welcome on plans for ensuring such safeguards are adopted and respected by all participants.

Finally, the CLD feels compelled to sound a note of caution regarding plans to make CSIF participation mandatory. The general experience of CLD members is that information sharing amongst sector participants consistently yields the most value when it occurs in a forum that is conducive to fostering openness and trust, and when it is animated by shared incentives.[6] The adoption of a "stick" versus a "carrot" approach for purposes of CSIF participation may pose some challenges to cultivating an environment in which sensitive information can be shared openly and efficiently. The CLD encourages the OEB to consider these and other potential issues further, and supports the solicitation of further guidance from the CSAC on this matter.

Cyber Security Advisory Committee ("CSAC")

The CLD supports the proposed formation of the CSAC and agrees that the establishment of such a body will help ensure industry ownership and accountability, while providing the OEB with valuable guidance and expertise on a range of issues related to Framework implementation.

As discussed above, the CLD strongly believes that the CSAC should be the central forum for subsequent discussion on possible approaches to future implementation and compliance activity.

E. CONCLUSION

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

[6] Successful examples in this regard include the IESO's Cyber Security Forum and NERC's Electricity Information Sharing and Analysis Center (or "E-ISAC").

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. The CLD looks forward to future engagement on this critical initiative.

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