EDA | POWER OF LOCAL HYDRO

The Voice of Ontario's Electricity Distributors

Ontario Energy Board
2300 Yonge St., 27th Floor
Toronto, ON M4P 1E4
Attn: Ms. K. Walli
Board Secretary

October 15, 2018

Dear Ms. Walli

Re: **EB-2016-0032**

The Electricity Distributors Association (EDA) thanks the Ontario Energy Board (OEB, the Board) for the opportunity to comment on its proposed amendments to the Reporting and Record Keeping Requirements (RRR) for Cyber Security readiness.

Ontario's Local Distribution Companies (LDCs) manage risks, like Cyber Security, on an ongoing basis and are experienced in protecting data and keeping systems secure from inappropriate access. They understand the benefits of providing well designed security and protection, and of testing for preparedness. LDCs prudently implement sound designs, whether proprietary or shared, and cost effectively secure and protect data (including system operating data, customer data and financial data) and systems from inappropriate access.

The EDA seeks to understand how the Board will use the data provided through the proposed RRRs and the range of actions that it may subsequently take (e.g., seek additional information, review cyber security systems, conduct an audit). The proposed RRRs implicitly require that LDCs interface their cyber security plans and practices with the OEB's Ontario Cyber Security Framework (Framework) to express their cyber risks and readiness using the Board's nomenclature. LDCs understand that the first report, that will be submitted in April 2019, will set the OEB's baseline understanding. The quality of this baseline reporting will improve if LDCs consistently report on the application of the cyber security tools provided by the Board. Without further support and guidance from the OEB there is a risk that two similarly prepared LDCs could report differently (e.g., depending on their respective level of conservatism).

Our LDC members acknowledge that the Framework will evolve over time. They are prepared that in future their risk profile may increase or that it may be appropriate for them to implement an increased number of mitigation tactics; for example, an LDC that previously indicated 'Implemented' in its 'Supporting Information' filed under the proposed Part 4, may under an evolved Framework report as 'Not Implemented' – and possibly for an extended period of time. The EDA seeks guidance from the Board about how it will accommodate these and other changes

Electricity Distributors Association
3700 Steeles Ave. W., Suite 1100, Vaughan, Ontario L4L 8K8 Tel/Fax 647.EDA.5300 1.877.262.8593 email@eda-on.ca www.eda-on.ca

and notes that all LDCs will benefit from clarity on the period of time available to implement change.

LDCs are preparing to evolve their cyber security readiness. Depending on an LDC's Risk Profile and the alignment between their current practices and the OEB's identified mitigations, the LDC may need to expend incremental resources or invest additional funds. They assume that the ongoing costs will be eligible for recovery through rates.

The EDA provides its detailed comments on the proposed changes in the enclosed Attachment and looks forward to supporting LDCs and the OEB in understanding and preparing for Cyber Security threats and risks. Please direct any questions to Kathi Farmer, the EDA's Senior Regulatory Affairs Advisor at kfarmer@eda-on.ca or at 905.265.5333.

Sincerely

Justin Rangooni
Vice-President, Policy and Government Relations

Encl.

Detailed comments on the Ontario Energy Board's proposed Reporting and Record Keeping Requirements on the Ontario Cyber Security Framework

Part 1 – 'General Information'

Local Distribution Companies (LDCs) note that the 'Cyber Security Contact Name' could be an individual with subject matter expertise or with administrative responsibility. The Electricity Distributors Association (EDA) suggests that in addition to providing information on the individual at the licensed distributor that the Ontario Energy Board (OEB, the Board) provide flexibility to name an individual at a third party for those instances where the LDC has contracted for the provision of cyber security, data protection, systems protection and other services. It may be helpful to expand the 'Self-Certification Statement' to root self-certification against the Ontario Cyber Security Framework (Framework). Lastly, LDCs seek confirmation that the period being reported on is the previous calendar year; if this is the case, LDCs suggest that the 'Self-Certification Statement' be amended to reflect that the data provided is specific to the end of the reporting period.

Part 2 – 'Request for Information'

No comments.

Part 3 – 'Acknowledgement of Status'

The EDA anticipates that for some LDCs the risk assessment tool will demonstrate that the LDC is simultaneously incurring 2 levels of risk. The EDA seeks guidance for our members as to how to complete this section of the form: whether they should use a conservative approach and select the highest level of risk identified through the Inherent Risk Profile Tool or proceed differently.

The 'Status of Implementation of Control Objectives' section attracted many comments. LDCs propose that the OEB clarify that the LDC is to select 'Some', 'All', or 'Exceed' based on their risk profile as identified using the Inherent Risk Profile Tool. The EDA also suggests that the OEB provide appropriate context when using the word 'plans' to clarify whether the LDC is to report that it has a formal and documented plan, or, is to report that is has taken or will take actions.

Each LDC will have a unique position on which 'Control Objectives' are 'critical'. The EDA seeks clarification that the OEB will use the data filed by LDCs to understand how an individual LDC is progressing over time, rather than to compare and contrast among LDCs. It is also unclear whether an LDC is expected to complete this section based on holistic findings such that it is appropriate to select one of 'Some', 'All' or 'Exceed', or at a more granular level where it could reasonably select more than one option. Whichever approach is intended our members point out that the OEB should communicate its thinking on how changes on a year over year basis will be dealt with (e.g., if an LDC that self-reports 'Exceed' in one year and 'Some' in the next year).

Those LDCs who plan to implement 'Control Objectives' seek information about the time available to complete the planned implementation and clarity about whether supporting documentation may be required.

Over time an LDC may alter its risk tolerance and, consequently, its 'Control Objectives' that will result in changes to the LDC's reported Status. LDCs would like to understand the OEB's thinking on how changing risk tolerance can impact Cyber Security preparedness generally and the 'Status of Implementation of Control Objectives' specifically.

The EDA also assumes that just as the Framework will evolve so will the OEB's Inherent Risk Profile Tool. We seek insight into how the OEB will deal with year over year self-reporting that documents a transition of risk, either an increase or a decrease, and whether the Board would initiate follow up actions. LDCs assume that the Inherent Risk Profile Tool that supports completing the 'Cyber Security Readiness Report' should be kept on record.

Part 4 – 'Supporting Information'

The EDA suggests that the questions be reworded to better align with the permitted responses; many of the questions as stated can be correctly answered with 'Yes' or 'No', rather than 'Implemented' or 'Not Implemented'. Alternatively, the responses offered may need to be augmented with the option of 'A Program is not in Place'. To improve consistency the EDA suggests that the OEB:

- cross reference each question to the relevant Self-Assessment Questionnaire; and
- clarify how an LDC that is developing or implementing aspects of cyber security readiness should complete each question to correctly convey the LDC's status or provide a third option (e.g., 'Implementation Pending', 'In Progress').

LDCs trust that their existing cyber security practices will be accepted as appropriate and cost effective. There is nonetheless an overarching question as to the Board's expectation for formal plans, assessment of risk tolerance, identification of mitigating strategies, associated decision making where the LDC may need to provide or invest in additional resources. The EDA presumes that these costs, like all other ongoing costs incurred to provide service at an appropriate level, will be eligible for recovery through rates.

The EDA is aware that the OEB has commenced a proceeding on LDC corporate governance. Among the suggestions made by the Board in that initiative is the expectation that good governance includes documentation of policies. The EDA seeks clarity from the Board as to how the proposals made in that OEB initiative interface with these Reporting and Record Keeping Requirements interface.

Below are the EDA's comments on specific questions. The EDA notes that the preamble to the questions makes reference to the period January 1 to December 31, 2018. The EDA assumes that these dates are provided for clarity only and that they will either be removed from the final version or will be updated annually.

Question 1 makes reference to a program without defining the term or describing a program. LDCs are familiar with the OEB's use of this term in the context of system planning and asset management. Our LDC members seek to understand this term accurately in the context of cyber security readiness.

Question 2, as worded, refers to operational risk decisions. This is broad and could, if applied liberally, envelope all aspects of the LDC's provision of service and resourcing. LDCs consider it appropriate to focus this question on operational risk decisions specific to:

- information;
- information management;
- information and systems security; and
- security.

Question 4 may be premature for the filing to be submitted April 30, 2019. LDCs note that the IESO's information sharing service is expected to be available in 2019.

Question 6 will benefit from including a text box so that the LDC can provide the date of the most recently provided training.

Question 7 is sensible on its own and, for reasons of completeness, likely should also be incorporated into Question 3. Please see the comments on Question 1.

Question 8 should read: 'Do you have appropriate systems and/or processes in place to identify, detect and protect against cyber security and privacy events/incidents?'.

Questions 9 and 11 should read: 'Do you have appropriate incident response processes and procedures in place for privacy and/or cyber security events/incidents? Are they documented?'.

Questions 10 and 12 will benefit from an additional check box suitable for LDCs who have not yet tested these processes and procedures.