Lakefront Utilities Inc.

October 15, 2018

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

Re: Proposed Cyber Security Readiness Report and Amendments to Electricity Reporting and Record Keeping Requirements RRR (Board File No.: EB-2016-0032)

Dear Ms. Walli:

Lakefront Utilities Inc. (LUI) distributes electricity to over 10,000 customers within its licensed service territory in the Town of Cobourg and the Village of Colborne, which is comprised of over 85% residential customers while approximately 12% are small business or industrial based.

Lakefront is pleased to provide input as the Ontario Energy Board (OEB) commences to develop the tools that will guide its oversight of the appropriate cyber security framework to be implemented by Ontario's LDCs. Cyber security is an evolving issue where the risk of unacceptable outcomes cannot be overstated or completely mitigated. Ontario's electricity LDCs are well aware of the importance of appropriately safeguarding customer and system information balanced by the need to support commercial transactions, facilitate markets, and fulfill government policy.

Lakefront has also discussed the proposed cyber security readiness report with its IT services provider, Horn IT Solutions Inc. and Collins Barrow Kawarthas Consulting Inc.

We trust this information and comments are beneficial to the Board as it continues its work to finalize this important initiative.

Yours truly,

Lakefront Utilities Inc.

Dereck C. Paul
President & CEO

Cc: Paul Cleary — Horn IT Solutions Inc.
Blair Brown, MSc, CISSP, CCE, ACE — Collins Barrow Kawarthas Consulting Inc.

Reporting on Assessment, Plans, and Progress

The Ontario Energy Board (OEB) intends to review the Cyber Reports from licensed transmitters and distributors to assess the state of readiness, and in order to develop a baseline in the sector's readiness. The review will assist in the consideration of a timeline by which all licensed transmitters and distributors will have implemented their plans to achieve the control objectives.

Lakefront notes that the changing environment is also important, the cyber landscape will change significantly, and the regulatory requirements expect to continuously adjust to this evolving environment. Consequently, utilizing the information obtained from the Cyber Reports to establish a timeline for all distributors, is unrealistic.

Part 4 (supporting information) requires the distributor to select the description that most closely reflect their efforts. The only options available are "Implemented" and "Not Implemented". The terms are subjective, leading to varied interpretations of differing responses. Compliance (selecting implemented) is not equal to effective security. Lakefront proposes that cyber security systems should be customized and specific to the applicable distributor and therefore more flexible in their application. Distributors continue to have unique risks, different threats, different vulnerabilities and different risk tolerances.

Further, the framework suggests that in the first stage of the regulation, there is no requirement for an external audit, only a self-attestation. As such, there will be discrepancies among the resulting requirements and implemented controls for entities which similar cyber security postures.

Protect

Question #7, enquires if a distributor has a program in place to address privacy and cyber security controls for 3rd party service providers.

The complex extended web of relationships with third-party suppliers and vendors is the lifeblood of many distributors today. Taking the steps to improve third-party risk management can provide peace of mind and continued success for the long term. The distributors program to address privacy and cyber security controls should provide for ongoing risk measurement and monitoring, performance measurement and monitoring, incident tracking, and evaluation of the value received from each relationship. These activities are important for determining when or whether to renegotiate agreements with third parties. The distributors most successful in this auditing and monitoring function are those that work to enhance the data they possess about their relationships so that they can predict areas of risk more accurately and automate relationship monitoring more effectively. Further, it's entirely possible to be compliant with the framework without having a software security program or reviewing the software security practices of the distributor's software vendors.

However, the requirement is unclear as to the specific program that is in place for 3rd party service providers. Further, when assessing third-party risk management, the OEB is dealing with a constantly evolving environment. As noted above, this create discrepancies between distributors.

Further, compliance item #7 would require each LDC to independently conduct evaluations or audits of their third party vendors. It should be recognized that since many of the LDCs commonly use the same vendors, this requirement would result in each LDC duplicating assurance efforts and compounding overall costs. It should also be recognized that third party vendors would be required t participate in multiple audits related to OEB Cyber Security, which could present an operational burden. To alleviate this duplication and the operational impacts of such an approach, Lakefront would recommend that a common audit and assurance standard be prepared for third-party vendors and their compliance be assured by a central authority.

Detect

Question #8 requires the distributor to identify if there are any systems and/or processes in place to identify, detect, and protect cyber security and privacy events/incidents.

Lakefront is concerned that the ambiguity of the term events/incidents will create discrepancies among the distributors. There is no guidance on what constitutes an "event/incident" and these terms are not consistent with other legislation, such as PIPEDA, where the term breach is used. Lakefront suggest that a common taxonomy of terms be issued for use in relation to cyber security analysis and reporting, such as NISTIR 7298.

Lakefront is also concerned with ensuring that requirements for event reporting are established in consideration of appropriate criticality and categorization thresholds.

Respond/Recover

Question #10 and Question #12 requires the distributor to identify of regular testing has been documented for event/incident response and recovery.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other processes.

Distributors will require more clarity regarding the key controls to be tested as part of the respond and recover phase. Distributors could establish risk-based testing or rotational testing consisting of self-assessment, desktop audits, on-site tests.

Lakefront suggests that the Ontario Energy Board provide a specific risk-based approach that integrates leading industry practices and standards to efficiently evaluate the design and operating effectiveness of controls over key IT security and cybersecurity areas.