Ontario Energy Board
P.O. Box 2319
27th Floor
2300 Yonge Street
Toronto ON M4P 1E4
Telephone: 416- 481-1967
Facsimile: 416- 440-7656
Toll-free: 1-888-632-6273

Commission de l'énergie de l'Ontario
C.P. 2319
27e étage
2300, rue Yonge
Toronto ON M4P 1E4
Téléphone: 416- 481-1967
Télécopieur: 416- 440-7656
Numéro sans frais: 1-888-632-6273

Ontario

BY EMAIL AND WEB POSTING

September 20, 2018

To: All Licensed Electricity Distributors
All Licensed Electricity Transmitters
All Participants in Consultation Process EB-2016-0032

Re: EB-2016-0032 –
Proposed Cyber Security Readiness Report & Amendments to Electricity Reporting and Record Keeping Requirements (RRR)

Background

On March 15, 2018, the Ontario Energy Board (OEB) issued a Notice of Amendments to the Transmission System Code and the Distribution System Code (Notice), which established regulatory requirements for licensed transmitters and distributors to provide the OEB with information on the actions they are taking relative to their cyber security risks. The Transmission System Code and the Distribution System Code were amended to require that a licensed transmitter or distributor provide the OEB with reports on its cyber security readiness referencing the Ontario Cyber Security Framework (Framework). The purpose of this letter is to provide stakeholders with the opportunity to comment on a proposed form of report on cyber security readiness (Cyber Report) that has been developed through discussions with the industry.

The purpose of the Cyber Report by licensed transmitters and distributors is to provide the OEB with information regarding a transmitter's or distributor's cyber security readiness, including its risk assessment and the status of implementation of control objectives relying on the Framework as a guide. By reporting on cyber security readiness against the Framework's consistent criteria, the OEB will have greater confidence that the reported state of cyber security in the electricity sector is comparable and understood. Distributors and transmitters are reminded that they bear responsibility for addressing

cyber security in the context of their enterprise risk and ensuring it achieves the OEB's expectations for reliability, security and privacy.

Cyber Security Report

The OEB reconvened the Cyber Security Working Group that had developed the Framework to advise OEB staff on the development of annual reporting requirements. The proposed Cyber Report (see Appendix 'A') is focused on the critical aspects of cyber security readiness identified in the industry developed Framework. The proposed Cyber Report is designed to require licensed transmitters and distributors to report on their assessment, plans and progress.

The OEB is proposing to require the Cyber Report to be filed annually as part of a transmitter's or distributor's reporting under the *Electricity Reporting and Record Keeping Requirements* (RRR). The Cyber Report will be required starting on April 30, 2019 and the OEB proposes to add sections 2.1.22 and 3.1.7 to the RRR to formalize the requirement (see Appendix 'B' for proposed amendments to the RRR).

The focus of the Cyber Report will be on the plans and timelines needed to address each licensed transmitter's and distributor's risk assessment and the progress in achieving their targeted state of cyber security readiness, as identified under the Framework. The 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 of the sector's readiness. This 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 that are appropriate for their operations.

The OEB acknowledges that cyber security reports received from licensed transmitters and distributors may contain sensitive information pertaining to the security of transmission and distribution systems. Therefore the OEB intends to treat the Cyber Reports as confidential under section 1.7 of the RRR.

Invitation to Comment

Interested parties are invited to provide comments on the proposed Cyber Report no later than October 15, 2018. Following its review of any comments received, the OEB will issue the revised RRR.

Cost awards will not be available under section 30 of the *Ontario Energy Board Act, 1998.*

Filing Instructions

All comments should be provided in writing to:

Board Secretary
Ontario Energy Board
P.O. Box 2319
2300 Yonge Street, Suite 2700
Toronto, Ontario, M4P 1E4

The OEB requests that interested parties make every effort to provide electronic copies of their comments in searchable/unrestricted Adobe Acrobat (PDF) format, and to submit their filings through the OEB's web portal at https://pes.ontarioenergyboard.ca/eservice/. A user ID is required to submit documents through the OEB's web portal. If you do not have a user ID, please visit the "e-filings services" webpage on the OEB's website at www.oeb.ca, and fill out a user ID password request.

Additionally, interested parties are requested to follow the document naming conventions and document submission standards outlined in the document entitled "RESS Document Preparation – A Quick Guide" also found on the e-filing services webpage. If the OEB's web portal is not available, electronic copies of filings may be filed by e-mail at registrar@oeb.ca.

Comments must be received by the Board Secretary by **4:45 p.m.** on October 15, 2018. They must quote file number EB-2016-0032 and include your name, address, telephone number and, where available, your e-mail address and fax number.

If the written comment is from a private individual (i.e., not a lawyer representing a client, not a consultant representing a client or organization, not an individual in an organization that represents the interests of consumers or other groups, and not an individual from a regulated entity), before making the written comment available for viewing at the OEB's offices or placing the written comment on the OEB's website, the OEB will remove any personal (i.e., not business) contact information from the written comment (i.e., the address, fax number, phone number, and e-mail address of the individual).

However, the name of the individual and the content of the written comment will be available for viewing at the OEB's offices and will be placed on the OEB's website.

Any questions should be directed to industryrelations@oeb.ca, or by phone at 416-314-2455 or 1-888-632-6273 (the OEB's toll-free number).

DATED at Toronto, **September 20, 2018**
ONTARIO ENERGY BOARD

Original signed by

Brian Hewson
Vice President,
Consumer Protection and Industry Performance

Appendix A:

Ontario

Cyber Security Readiness Report

All information submitted in this process will be used by the OEB solely for the purpose of assessing the industry's cyber security readiness. All submitted information will be kept confidential.

PART 1 – GENERAL INFORMATION	
Licensee Name:	
Licensee ID:	
Cyber Security Contact Name[1]**:**	
Cyber Security Contact Telephone No.:	
Cyber Security Contact E-mail:	
Self-Certification Statement: I attest to the reported cyber security readiness outlined in this report for the licensee as of the report completion date.	
Chief Executive Officer (CEO) Name:	
CEO Signature:	
Date CEO Signed:	

PART 2 – REQUEST FOR INFORMATION

Pursuant to the "*Electricity Reporting and Record Keeping Requirements"*, licensees are required to provide the OEB with information on cyber security readiness and actions they are taking relative to their cyber security risks.

Using the Ontario Cyber Security Framework (Framework), licensees are expected to assess their own risk tolerance in determining the control objectives they plan to achieve. This information is to be provided by completing Part 3 and Part 4 of this form.

PART 3 - ACKNOWLEDGEMENT OF STATUS

Signatory(s) confirms:

I have read and understand the Framework and in applying the self-assessment steps using the Inherent Risk Profile Tool, my organization's risk would be rated as:	☐ HIGH ☐ MEDIUM ☐ LOW

[1] The Cyber Security Compliance Contact is the individual at your organization who would be contacted about a cyber security update.

Status of Implementation of Control Objectives consistent with my Organization's Risk Profile		
PLANS TO IMPLEMENT SOME CONTROL OBJECTIVES	☐	Control objectives critical to my organization are implemented.
	☐	Control objectives critical to my organization are planned to be implemented within ___ years.
PLANS TO IMPLEMENT ALL CONTROL OBJECTIVES	☐	Control objectives defined in the Framework are implemented.
	☐	Control objectives defined in the Framework are planned to be implemented in ___ years.
PLANS TO EXCEED CONTROL OBJECTIVES	☐	Additional control objectives critical to my organization have been implemented.
	☐	Additional control objectives critical to my organization are planned to be implemented in ___ years.

PART 4 - SUPPORTING INFORMATION – CYBER SECURITY

Please answer the following questions by selecting the check box that most closely reflects your efforts.

Status report for the period from January 1, 2018 to December 31, 2018:

IDENTIFY	
1. Do you have a corporate privacy and cyber security governance[2] program in place?	☐ Implemented ☐ Not implemented
2. Based on your organization's risk profile, do you have privacy and cyber security risk identification and risk prioritization processes in place to support your operational risk decisions?	☐ Implemented ☐ Not implemented

[2] Governance: The policies, procedures, standards and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the senior management of privacy and cyber security risk - see OEB NIST Privacy Security Controls Self-Assessment Questionnaire

3. Do you undergo 3rd party and/or self-audits/assessments[3] of your privacy and cyber security program based on your organization's risk profile? Please check all that apply.	**3rd Party Audits/Assessments:** ☐ Implemented ☐ Not implemented **Self-Audits/Assessments:** ☐ Implemented ☐ Not implemented
4. Do you actively participate in one or more of the IESO's information sharing services?	**Cyber Security Situational Awareness** ☐ Actively Using Information ☐ Not Using Information **Information exchange** ☐ Actively Participating ☐ Not Participating
PROTECT	
5. Do you have **mitigation** plans in place for your organization's privacy and cyber security risk areas based on your 3rd party or self-assessment?	☐ Implemented ☐ Not implemented
6. Do you have a privacy and cyber security awareness education and training program in place for the organization's personnel and partners to perform their information security-related duties and responsibilities consistent with related policies, procedures, standards and agreements[4]?	☐ Implemented ☐ Not implemented
7. Do you have a program in place to address privacy and cyber security controls for 3rd party service providers?	☐ Implemented ☐ Not implemented
DETECT	
8. Do you have systems and/or processes in place to identify, detect and protect cyber security and privacy events/incidents?	☐ Implemented ☐ Not implemented

[3] Refer to the auditing section of the Framework (page 18).
[4] OEB NIST Privacy Security Controls Self-Assessment Questionnaire

RESPOND	
9. Do you have documented incident **response** processes and procedures in place for privacy and cyber security events/incidents?	☐ Implemented ☐ Not implemented
10. Are you regularly testing your documented event/incident **response** processes and procedures for privacy & cyber security?	☐ Implemented ☐ Not implemented
RECOVER	
11. Do you have documented incident **recovery** processes and procedures in place for privacy and cyber security events/incidents?	☐ Implemented ☐ Not implemented
12. Are you regularly testing your documented event/incident **recovery** processes and procedures for privacy & cyber security?	☐ Implemented ☐ Not implemented

Appendix B:

Amendments to the Electricity Reporting and Record Keeping Requirements

Note: The text of the amendments is set out in italics below, for ease of identification.

1. Section 2.1.22 is added after section 2.1.21:

   2.1.22: *A distributor shall provide, in the form and manner required by the Board, annually, by April 30, the following information:*

   a. *the status of cyber security readiness, as required by section 6.8.1.1 of the Distribution System Code; and*
   b. *a self-certification statement signed by the Chief Executive Officer on the reported cyber security readiness, as required by section 6.8.1.2 of the Distribution System Code.*

2. Section 3.1.7 is added after section 3.1.6:

   3.1.7: *A transmitter shall provide, in the form and manner required by the Board, annually, by April 30, the following information:*

   a) *the status of cyber security readiness, as required by section 3B.2.2.1 of the Transmission System Code; and*
   b) *a self-certification statement signed by the Chief Executive Officer on the reported cyber security readiness, as required by section 3B.2.2.2 of the Transmission System Code.*

3. Section 1.7 is amended as follows:

   1.7: *Add section 2.1.22 under 'Distributor' and add section 3.1.7 under 'Transmitter'.*