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

November 29, 2018

To: All Licensed Electricity Distributors
All Licensed Electricity Transmitters

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

On September 20, 2018, the Ontario Energy Board (OEB) issued for comment proposed Amendments to the *Electricity Reporting and Record Keeping Requirements (RRR)* for licensed transmitters and distributors (licensees) and a proposed Cyber Security Readiness Report (Cyber Report). The purpose of this letter is to inform licensees that the OEB has adopted the Cyber Report and Sections 2.1.22 and 3.1.7 to the RRR, which are set out in Appendices A and B, respectively. Licensees are required to submit their first Cyber Report by April 30, 2019.

Background

The new reporting requirements follow from the Amendments to the Transmission Systems Code and Distribution System Code in March 2018 that established the OEB's expectations regarding licensees' cyber security readiness and the requirements that licensees use the Ontario Cyber Security Framework (Framework) as the basis for reporting on their cyber security readiness. The Cyber Report is intended to provide information to the OEB regarding a licensees' implementation of the Framework's risk assessment and the status of control objectives.

In response to the September 2018 letter, the OEB received comments from the Coalition of Large Distributors, Lakefront Utilities Inc., PUC Distribution Inc. and the Electricity Distributors Association. Comments received supported the proposals in the letter although some stakeholders suggested the need for additional clarifications. The

OEB has considered the comments and made certain revisions[1] to the Cyber Report that is attached as Appendix A.

Stakeholder comments included a request for the ability to provide commentary to allow for additional explanation in Part 4 of the Cyber Report. The intention of the Cyber Report is to confirm to the OEB whether a licensee has implemented the identified activities related to cyber security readiness.

The OEB will use this information to both assess the sector and individual licensee's state of readiness in order to determine if any further action is necessary. Therefore the OEB only requires the licensee's statement about its implementation and not the details, which may include sensitive information that is not needed for the initial assessment. The information contained in the Cyber Report will be sufficient to enable the OEB to develop a baseline of the electricity sector's cyber security readiness.

Some stakeholders asked for clarity as to how changes in the Framework will be addressed as part of the reporting on cyber readiness. The OEB acknowledges that the industry-led Framework will evolve to integrate key learnings over time, and this will require licensees to make appropriate adjustments and assess their plans. Likewise, the OEB will assess if the evolutionary changes necessitate any adjustments to the Cyber Report.

Two stakeholders requested guidance on how to report that their organization was in a transitional range, as identified in the Framework. The transitional ranges, 'Low to Medium' and 'Medium to High', are included in the Framework to provide utilities with the flexibility to choose the risk profile that best matches their unique situation in assessing their cyber security readiness. However, the transitional ranges do not need to be reported to the OEB as part of the assessment of whether the licensee has completed the actions identified in the Cyber Report.

One stakeholder suggested separate reporting on the status of implementation efforts related to cyber security and privacy, as these activities may be carried out separately within the organization. Privacy and security of consumer information has been incorporated into the industry-developed Framework based on best practices and it would lead to potential duplication and inefficiencies to have separate reports.

Stakeholders expressed concerns about the costs related to implementing control objectives in the Framework. As the OEB previously expressed in the December 2017 Notice licensees are expected to incorporate cyber security investments into their transmission or distribution system plans and that these responsibilities should be

[1] Revisions: Reporting instructions. Footnotes: Cyber Security Contact Name, Cyber Governance, Cyber Incidents & Cyber Events.

addressed in the same manner as any other operational risks.

The OEB is using this opportunity to clarify, in response to comments, that a response of “Not Implemented” to questions 1 through 12 of the Cyber Report does not mean the licensee is not compliant with the requirements under the Codes.

Implementation

The new sections of the RRR come into effect immediately and licensees will be required to submit their first annual Cyber Report as of April 30, 2019. Instructions for the completion and filing of the reports will be set out in the OEB’s Reporting and Record Keeping Requirements (RRR). Any questions should be directed to IndustryRelations@oeb.ca, or by phone at 1-877-632-2727.

DATED at Toronto, **November 29, 2018**

ONTARIO ENERGY BOARD

Original signed by

Brian Hewson
Vice President,
Consumer Protection and Industry Performance

Attachments:
Appendix A – Cyber Security Readiness Report
Appendix B – Amendments to the Electricity Reporting and Record Keeping Requirements

Appendix A:

Cyber Security Readiness Report

All information submitted in this process will be kept confidential and used by the OEB solely for the purpose of assessing the industry's cyber security readiness. **PART 1 – GENERAL INFORMATION**	
Licensee Name:	
Licensee ID:	
Cyber Security Contact Name:[2]	
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 shall identify the control objectives that would apply to their organization in accordance with their Inherent Risk Profile.

Licensees are expected to determine the control objectives that they plan to implement and how they will be achieved based upon their assessment of their organization's cyber security risk tolerance. This information is to be provided by completing Part 3 and Part 4 of this form.

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

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

Licensees to select one check box ☐ in the categories 'Some', 'All', or 'Exceed' based on your risk profile, as identified using the Inherent Risk Profile Tool.

PART 4 - SUPPORTING INFORMATION – CYBER SECURITY

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.

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 program[3] in place?	☐ Implemented ☐ Not implemented

[3] NIST SP 800-100 – Effective Information Security Governance Program. p.14

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
3. Do you undergo 3rd party and/or self-audits / assessments[4] 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?[5]	☐ Implemented ☐ Not implemented

[4] Framework – Auditing p.18
[5] NIST Privacy Security Controls Self-Assessment Questionnaire

DETECT	
7. Do you have systems and/or processes in place to identify, protect and detect cyber security and privacy events/incidents?[6]	☐ Implemented ☐ Not implemented
RESPOND	
8. Do you have documented incident **response** processes and procedures in place for privacy and cyber security events/incidents?	☐ Implemented ☐ Not implemented
9. Are you regularly testing your documented event/incident **response** processes and procedures for privacy & cyber security?	☐ Implemented ☐ Not implemented
RECOVER	
10. Do you have documented incident **recovery** processes and procedures in place for privacy and cyber security events/incidents?	☐ Implemented ☐ Not implemented
11. Are you regularly testing your documented event/incident **recovery** processes and procedures for privacy & cyber security?	☐ Implemented ☐ Not implemented

[6] NISTR – 72.98r2 – p.57 "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein." NIST SP800-61r2 – Cyber Security Incident Handing Guide - p.6 "computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

Appendix B:

Amendments to the Electricity Reporting and Record Keeping Requirements (RRR)

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'.*