Ontario Energy Board | Commission de l'énergie de l'Ontario

BY EMAIL AND WEB POSTING

CYBER SECURITY READINESS REPORT & NOTICE OF AMENDMENTS TO THE NATURAL GAS REPORTING AND RECORD KEEPING REQUIREMENTS (RRR) RULE FOR GAS UTILITIES BOARD FILE NO.: EB-2016-0032

To: All Natural Gas Utilities
All Other Interested Parties

Date: April 25, 2019

The Ontario Energy Board (OEB) is giving notice under Section 45 of the *Ontario Energy Board Act, 1998* (OEB Act) of amendments to the *Natural Gas Reporting and Record Keeping Requirements (RRR) Rule for Gas Utilities* (Rule).

A. Background

On March 14, 2019, the Ontario Energy Board (OEB) issued a Notice of Proposed Amendments to the Rule, and a Cyber Security Readiness Report (Cyber Report) for comment.

On February 11, 2016, the OEB initiated a consultation to review cyber security and data privacy in relation to licensed electricity transmitters and distributors (EB-2016-0032). The OEB codified cyber security reporting obligations through amendments[1] to the TSC, DSC, and the Reporting and Record Keeping Requirements for the electricity sector.[2]

In January 2018, the OEB established a Working Group for the rate-regulated gas utilities (Utilities), as a natural progression from the electricity-related amendments. The OEB consulted with the Working Group regarding development of cyber security, privacy protection for consumers and the refinement of cyber reporting requirements for the gas sector.

---

[1] TSC & DSC Amendments
[2] Reporting & Record Keeping Requirements

In those discussions, the Utilities advised the OEB that they have established programs and have adopted a risk-centric approach to cyber security, including the use of industry best practices that differ from the electricity sector. The Utilities also recommended adoption of their existing security management programs (Cyber Security Program) as the preferred basis for readiness reporting. This approach, in the Utilities' view, avoids duplication of effort and enables each Utility to develop and mature its internal policies to best satisfy its requirements. The OEB accepted this approach as being the most pragmatic and efficient means of ensuring the reporting will provide a meaningful assessment of a Utility's cyber-readiness.

The proposed reporting requirements adopted the Utilities' existing cyber security management programs (Cyber Security Program) as the preferred basis for reporting to the OEB on their cyber security readiness. The Cyber Report will establish regulatory requirements for natural gas utilities (Utilities) to provide the OEB with information on the actions they are taking relative to their cyber security readiness.

B. Stakeholder Comments and Amendment

In response to the March 14, 2019 Notice, the OEB received comments from one stakeholder (Enbridge Gas Distribution, referred to below as Enbridge) on the proposed amendments to the Rule.

The OEB has considered the stakeholder comments and has made minor revisions to Sections 1.2, 1.6, 1.8 and 2.1.22 of the RRR, and to the form of Cyber Report. The revisions are set out in Appendices A and B, respectively.

The stakeholder comments are discussed below.

1. Revised Cyber Security Definition

The March 2019 Notice proposed to amend Rule by adding the following definition of Cyber Security:

> *"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access. Cyber Security includes both electronic and physical security.*

Enbridge suggested the removal of redundant information in the definition of Cyber Security and proposed the following two (2) options for the definition:

a. *"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access*; or

b. *"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access from both electronic and/or physical sources.*

The OEB has reviewed the comments and has adopted the second option suggested by Enbridge.

2. Self-Certification Statement

The March 2019 notice proposed that the Chief Executive Officer sign a self-certification statement on cyber security readiness. Enbridge, as outlined in the comment below, suggested an adjustment be made to the self-certification statement to better reflect internal protocols and include the ability for a Chief Information Security Officer (CISO) to enable cyber security certification reporting:

> *"It would be more reflective of internal protocols if the proposed amendment to Section 2.1 of the RRR Rule to require a self-certification statement on cyber security readiness be [sic] signed by the Chief Executive Officer was revised to also require that the self-certification statement be signed by the Chief Information Security Officer."*

The OEB has considered this recommendation and the OEB agrees that it is appropriate to have both the CISO and the CEO execute the self-certification statement. Section 2.1 of the RRR Rule has been revised to reflect this change.

3. Record Retention

Enbridge asked how long the OEB intends to retain the annual cyber security-related filings in its records. The OEB intends to maintain the related filings for at least 6 years from the end of the last calendar year to which the records relate.

The OEB has considered the stakeholder comments and made certain revisions to the Amendments attached as Appendix A.

C. Coming into Force

The new sections of the RRR come into force effective immediately and Gas Utilities are required to submit their first Cyber Report by **April 30, 2020**. Instructions for the completion and filing of the reports will be set out in the OEB's Reporting and Record Keeping Requirements (RRR). Questions should be directed to IndustryRelations@oeb.ca, or by phone at 1-877-632-2727.

DATED at Toronto, **April 25, 2019**

ONTARIO ENERGY BOARD

Original signed by

Brian Hewson
Vice President,
Consumer Protection and Industry Performance

Attachment A: Final Amendments to the Natural Gas Reporting and Record Keeping Requirements (RRR) Rule for Gas Utilities
Attachment B: Comparison Version of the Final Amendments to the Natural Gas Reporting and Record Keeping Requirements (RRR) Rule for Gas Utilities
Attachment C: Final Cyber Security Readiness Report – Gas Utilities

Attachment A
to
Notice of Amendments to a Rule
April 25, 2019
EB-2016-0032
Final Amendments to the Natural Gas Reporting and Record Keeping Requirements (RRR) – Rule for Gas Utilities

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

1. Section 1.2 is amended by adding the following definitions (in the proposer place based on alphabetical order):

> *"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access from both electronic and/or physical sources. Cyber Security includes both electronic and physical security.*
>
> *"Cyber Security Program" means the utility's internal Gas Cyber Security Program, which includes a methodology to assess risk, define benchmark objectives and measure cyber security readiness.*

2. Section 1.6 is amended to include information filed under section 2.1.22 among the information the OEB intends to treat as confidential. More particularly, the list of sections set out in section 1.6 is amended as follows:

> 2.1.3 (b), 2.1.22, 2.3.1, 2.3.5(a), 2.3.7.2 (a), (c) to (e), 2.3.8, 2.3.9, 2.3.10, 2.3.14 and 2.3.17.

3. Section 1.8 is amended to add the following paragraph to the end of the section: The amendments to section 1.2 (definitions of "Cyber Security", and "Cyber Security Program") and section 1.6, and the new section 2.1.22 of this Rule, made by the Board on April 30, 2019, come into force on April 30, 2019 and are applicable to all filings due on or after that date.

4. Section 2.1 is amended by adding the following paragraph: 2.1.22 A utility shall provide, in the form and manner required by the Board, annually, by the last day of the fourth month after the financial year-end, the following information for the preceding calendar year with respect to cyber security:

a) Information on cyber security readiness and actions it is taking relative to its cyber security risks.
b) A self-certification statement signed by the Chief Executive Officer (CEO) and the Chief Information Security Officer (CISO) on the reported cyber security readiness.

Attachment B
to
Notice of Amendments to a Rule
April 25, 2019
EB-2016-0032
Comparison Version of the Final Amendments
Final Amendments to the Natural Gas Reporting and Record Keeping Requirements (RRR) – Rule for Gas Utilities

Note: The text highlighted in red identifies the changes, for ease of identification.

1. Section 1.2 is amended by adding the following definitions (in the proposer place based on alphabetical order):

> *"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access from both electronic and/or physical sources. Cyber Security includes both electronic and physical security.*
>
> *"Cyber Security Program" means the utility's internal Gas Cyber Security Program, which includes a methodology to assess risk, define benchmark objectives and measure cyber security readiness.*

2. Section 1.6 is amended to include information filed under section 2.1.22 among the information the OEB intends to treat as confidential. More particularly, the list of sections set out in section 1.6 is amended as follows:

> 2.1.3 (b), 2.1.22, 2.3.1, 2.3.5(a), 2.3.7.2 (a), (c) to (e), 2.3.8, 2.3.9, 2.3.10, 2.3.14 and 2.3.17.

3. Section 1.8 is amended to add the following paragraph to the end of the section: The amendments to section 1.2 (definitions of "Cyber Security", and "Cyber Security Program") and section 1.6, and the new section 2.1.22 of this Rule, made by the Board on April 30, 2019, come into force on April 30, 2019 and are applicable to all filings due on or after that date.

4. Section 2.1 is amended by adding the following paragraph: 2.1.22 A utility shall provide, in the form and manner required by the Board, annually, by the last day of the fourth month after the financial year-end, the following information for the preceding calendar year with respect to cyber security:

a) Information on cyber security readiness and actions it is taking relative to its cyber security risks.
b) A self-certification statement signed by the Chief Executive Officer (CEO) and the Chief Information Security Officer (CISO) on the reported cyber security readiness.

Attachment C
April 25, 2019
EB-2016-0032

Cyber Security Readiness Report – Gas Utilities

Ontario Energy Board | Commission de l'énergie de l'Ontario

All information submitted in this process will be used by the OEB solely for the purpose of assessing the gas industry's cyber security readiness against utilities' internal Cyber Security Programs. 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:[3]	
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 utility as of the report completion date.	
Chief Executive Officer (CEO) Name:	
CEO Signature:	
Chief Information Security Officer (CISO) Name:	
CISO Signature:	
Date Signed:	

PART 2 – REQUEST FOR INFORMATION

Pursuant to the "Natural Gas Reporting and Record Keeping Requirements", utilities are required to provide the OEB with information on cyber security readiness and actions it is taking relative to its cyber security risks. Utilities are expected to apply their internal Cyber Security Program to determine the control objectives it plans to achieve and reflect on its own risk management approach to establish its objectives.

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

PART 3 – REQUEST FOR INFORMATION

PLEASE ANSWER THE FOLLOWING QUESTIONS BY SELECTING THE CHECKBOX THAT MOST CLOSELY REFLECTS YOUR EFFORTS. STATUS REPORT FOR THE PERIOD FROM JANUARY 1, 2019, TO DECEMBER 31, 2019:

IDENTIFY	
1. Do you have a corporate privacy and cyber security governance 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
3. Do you undergo 3rd party and/or self-audits / assessments 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 cyber security risk information sharing services? IESO's information sharing services?[4]	**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?	☐ Implemented ☐ Not implemented

[4] Information Sharing Services: ONG-ISAC, DNG-ISAC, AGA, CGA, INGAA, and CCIRC.

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, protect and detect cyber security and privacy events/incidents?[5]	☐ Implemented ☐ Not implemented
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

[5] NISTR – 72.98r2 – p.57, NIST SP800-61r2 –p.6