**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**

March 14, 2019

# NOTICE OF PROPOSED AMENDMENTS TO A RULE THE NATURAL GAS REPORTING AND RECORD KEEPING REQUIREMENTS (RRR) RULE FOR GAS UTILITIES EB-2016-0032

**To: All Natural Gas Utilities**
**All Other Interested Parties**

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

The purpose of the proposed amendments is to 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.

The OEB is seeking comments from stakeholders on the proposed amendments to the Rule until April 4, 2019.

## Background

On February 11, 2016, the OEB initiated a consultation to review cyber security and data privacy in relation to licensed electricity distributors and transmitters (EB-2016-0032). The OEB established cyber security reporting requirements for licensed electricity distributors and transmitters through amendments[1] to the OEB's Transmission System Code and Distribution System Code, and to the Electricity Reporting and Record Keeping Requirements.

[1] TSC and DSC Amendments.

The OEB established a Working Group for the Utilities in January 2018, as a further step in addressing cyber security in the energy sector. The OEB consulted with the Working Group to discuss the next steps as they related to cyber security, and more particularly to refining customer privacy and defining cyber security reporting requirements for the natural gas sector.

In those discussions, the Utilities advised that they have established cyber security programs and have adopted a risk-based approach to cyber security, including the use of industry best practices that differ from the approach in the electricity sector.

The Utilities also recommended adoption of their existing internal cyber security management programs (Cyber Security Program) as the preferred basis for reporting to the OEB. This approach, in the Utilities' view, avoids duplication of effort and allows each Utility to develop and mature its internal policies to best suit its needs. The OEB accepts this approach as being the most practical and efficient means of ensuring the reporting will provide a meaningful assessment of a Utility's cyber-readiness.

The Utilities also expressed support for a self-assessment attestation approach, similar to that required of electricity distributors and transmitters. The OEB views cyber security reporting for the gas sector as important and recognizes that the Utilities' approach to cyber-readiness is both Utility-specific and, according to the Utilities, incorporates industry best practices. Each Utility to which the RRRs apply is accountable to address cyber security in the context of its enterprise risk.

**Proposed Amendments to Natural Gas Reporting and Record Keeping Requirements (RRR) Rule for Gas Utilities**

The OEB's Proposed Amendments to the Rule are provided in Attachment A.

The Proposed Amendments require that each Utility report to the OEB on the status of cyber security readiness referencing its Cyber Security Program, at such times and in such a manner as may be directed by the OEB. In order to support the proposed RRR amendments, the OEB is proposing to add definitions of "Cyber Security" and "Cyber Security Program" to the Rule.

In order to facilitate reporting by the Utilities, the OEB is providing the form of the report that Utilities will be required to file annually on their assessment of cyber security readiness. The proposed Cyber Security Readiness Report for Utilities is provided in Attachment B and includes a self-certification by the Utility. Self-certification of cyber security capability by Utilities would be required annually starting April 30, 2020.

**Sensitive Information**
The OEB acknowledges that cyber security reports received from Utilities may contain sensitive information. The OEB does not intend to disclose the self-certification status of Utilities as part of public filings. The OEB intends to keep the reports as confidential and will segregate them from other records. Access will be limited to individuals within the OEB who require this information as part of their duties and work assignments.

The OEB is, therefore, proposing to amend section 1.6 of the Rule by including the material filed under the new section 2.1.22 among the information that the OEB intends to keep confidential.

**Effective Date**
The amendments to the RRR, as set out in Attachment A, will be effective the day the final amendments are posted on the OEB's website.

The first reporting under these sections will be due on April 30, 2020.

**Cost Awards**
Cost awards will not be available under Section 30 of the Act.

**Invitation to Comment**
Anyone interested in providing written comments on the proposed RRR amendments in Attachment A and the proposed Cyber Security Report in Attachment B is invited to submit them by April 4, 2019.

Your written comments must be received by the Board Secretary by 4:45 p.m. on the required date. 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.

One paper copy of your written comments must be provided and should be sent to:

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

The OEB requests that you make every effort to provide electronic copies of your written comments in a searchable/unrestricted Adobe Acrobat (PDF) format, and to submit them 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.

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

Those that do not have internet access should provide a USB flash drive containing their written comments in PDF format. 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), the OEB will remove any personal (i.e., not business) contact information from those written comments (i.e., address, fax number, phone number, and e-mail address) before making the written comment available for viewing at the OEB's offices or posting it on the OEB's website. However, the private individual's name 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.

This Notice, including all attachments, and all related written comments received by the OEB will be available for public viewing on the OEB's website at www.oeb.ca and at the OEB's office during normal business hours.

If you have questions regarding these amendments, please contact industryrelations@oeb.ca or 1-888-632-6273 (toll-free within Ontario).

**DATED** at Toronto, March 14, 2019

**ONTARIO ENERGY BOARD**

*Original signed by*

Brian Hewson
Vice President,
Consumer Protection and Industry Performance

Attachment A: Proposed Amendments to the Natural Gas Reporting and Record Keeping Requirements (RRR) Rule for Gas Utilities
Attachment B: Proposed Cyber Security Readiness Report for Gas Utilities

## Attachment A:

## Proposed Amendments to the Natural Gas Reporting and Record Keeping Requirements (RRR) – Rule for Gas Utilities
## March 14, 2019

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

1. Section 1.2 is amended by adding the following definitions (in the proper 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. 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 on the reported cyber security readiness.*

## Attachment B:

## Cyber Security Readiness Report
## For Gas Utilities
## (DRAFT FOR COMMENT)

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 submitted information will be kept confidential.

| **PART 1 – GENERAL INFORMATION** | |
|---|---|
| **Utility Name:** | |
| **Utility ID:** | |
| **Cyber Security Contact Name:**[2] | |
| **Cyber Security Contact Telephone No.:** | |
| **Cyber Security Contact E-mail:** | |
| **Self-Certification Statement:**<br>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:** | |
| **Date CEO 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.

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

**PART 3 - SUPPORTING INFORMATION – CYBER SECURITY**

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 corporate privacy and cyber security governance program in place? | ☐ Implemented<br>☐ 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<br>☐ 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?<br><br>Please check all that apply. | **3rd Party Audits/Assessments:**<br>☐ Implemented<br>☐ Not implemented<br>**Self-Audits/Assessments:**<br>☐ Implemented<br>☐ Not implemented |
| **4.** Do you actively participate in one or more of the cyber security risk information sharing services?[3] | **Cyber Security Situational Awareness**<br>☐ Actively Using Information<br>☐ Not Using Information<br>**Information exchange**<br>☐ Actively Participating<br>☐ 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<br>☐ Not implemented |

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

| | |
|---|---|
| **6.** Do you have 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<br>☐ Not implemented |
| **7.** Do you have a program in place to address privacy and cyber security controls for 3rd party service providers? | ☐ Implemented<br>☐ Not implemented |
| **DETECT** | |
| **8.** Do you have systems and/or processes in place to identify, protect and detect cyber security and privacy events/incidents?[4] | ☐ Implemented<br>☐ Not implemented |
| **RESPOND** | |
| **9.** Do you have documented incident **response** processes and procedures in place for privacy and cyber security events/incidents? | ☐ Implemented<br>☐ Not implemented |
| **10.** Are you regularly testing your documented event/incident **response** processes and procedures for privacy & cyber security? | ☐ Implemented<br>☐ Not implemented |
| **RECOVER** | |
| **11.** Do you have documented incident **recovery** processes and procedures in place for privacy and cyber security events/incidents? | ☐ Implemented<br>☐ Not implemented |
| **12.** Are you regularly testing your documented event/incident **recovery** processes and procedures for privacy & cyber security? | ☐ Implemented<br>☐ Not implemented |

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