Tania Persad
Senior Legal Counsel

tel 416 495 5891
egdregulatoryproceedings@enbridge.com

Enbridge Gas Distribution
500 Consumers Road
North York, Ontario M2J 1P8
Canada

VIA RESS, EMAIL and COURIER

July 17, 2017

Ms. Kirsten Walli
Board Secretary
Ontario Energy Board
2300 Yonge Street, 27th Floor
Toronto, Ontario
M4P 1E4

Dear Ms. Walli:

Re: Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario – Board File No. EB-2016-0032

This is in response to the June 1, 2017 letter (Letter) from the Ontario Energy Board (OEB or Board) inviting comments from interested stakeholders by July 15, 2017 on the Staff Report to the Board on a proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors (Staff Report) and the accompanying industry developed Cyber Security Framework (Framework). Enbridge Gas Distribution Inc. (EGD) contacted Board Staff to request submission by today (as July 15 is a Saturday) and Board Staff granted this request. EGD is pleased to have the opportunity to provide these comments as a part of the large and complex Enbridge Inc. (Enbridge) organization that devotes significant time and resources to its cyber security systems.

Background

As noted in the Staff Report, EGD representatives answered cyber security survey questions issued by the Board and also participated in the two consultative groups established, including the Cyber Security Steering Committee and the Cyber Security Working Group (CSWG). Throughout this process, EGD understood that the primary focus was on Ontario's electricity distributors and the electric smart grid (Smart Grid). The Letter on page 3 also notes that the Staff Report outlines Staff's views on "the expectations for Ontario's electricity distributors regarding cyber security and privacy…" and does not identify gas distributors specifically. Further, the Staff Report states on page i, "Although the main [the] focus of the policy consultation to date has been on electricity distribution, OEB Staff is of the opinion that the proposed framework and reporting requirements may also apply to non-bulk transmission and gas distribution."

It is therefore not clear to EGD what the Board's intentions are with respect to applying the Staff Report and the Framework to gas distributors such as EGD.

In order to make a rule applicable to gas distributors, the OEB must follow the procedures set out in sections 44 and 45 of the *Ontario Energy Board Act, 1998* (OEB Act). The Board's rule-making powers with respect to gas distributors are more limited than its powers with respect to imposing conditions on licenses for electricity distributors and are restricted to the topics set out in section 44 of the OEB Act. The Staff Report does not specify how the Framework would apply to gas distributors nor does it explain how issues related to the Smart Grid may or may not apply to gas distributors. This topic was also not discussed in any detail in the consultative sessions that EGD attended. This is a complex topic that would warrant in-depth discussions before the Board or gas distributors could determine the full impact of the Framework on gas distributors and the systems that are currently in place. EGD would welcome such discussions.

In order to mandate application of the Staff Report and Framework to gas distributors, the Board must be explicit about its intention and legislative authority in this regard. Further, the Board must provide information about the anticipated costs and benefits of the proposed rule. None of this information has been provided by the Board in the Letter and EGD therefore assumes that it is not the Board's intention at this time to apply the Framework to gas distributors. As a participant in the Steering Committee and CSWG and a key stakeholder in the Ontario energy industry, EGD provides the following preliminary comments about the Framework in relation to how EGD, Enbridge and its subsidiaries manage cyber security risks today.

<u>Enbridge Cyber Security Systems</u>

EGD, and now Union Gas Limited (Union), are wholly owned subsidiaries of Enbridge, a leading North American energy delivery company with businesses in over 40 of the United States and 8 Canadian Provinces. As described in more detail in the Union submissions, Enbridge manages cyber security at the enterprise level in order to ensure that all of its many subsidiary companies, including EGD and Union, are meeting strong enterprise standards. EGD adopts Union's submissions in this regard and will not repeat those comments except to highlight EGD's primary observations with respect to the Staff Report and Framework.

In 2016, Enbridge developed and implemented a risk-based cyber security control framework to manage its cyber security risks and measure the effectiveness of controls. It was developed to address cyber security threats unique to Enbridge and in keeping with best practice; it applies the relevant components of external frameworks including those of the National Institute of Standards in Technology (NIST) and the Center for Internet Security (CIS) standard, Control Objectives for Information and Related

Technologies (COBIT) and Payment Card Industry (PCI) standards. It further applies the Enbridge Enterprise Risk Framework and produces a controls framework that provides a higher granularity focus on cyber security risks and threats specific to Enbridge and establishes Enbridge's cyber security risk tolerance levels, which in turn allows management to be disciplined with cyber security investments.

The outcome of this work was the development of controls that provide greater granularity on the existing Enbridge cyber security standards and three policies that have governed the program since 2015. The controls can be categorized as technical controls (automation i.e., firewalls), operational controls (process and automation i.e., vulnerability management), and operational and process controls (i.e., technology change control).

This collection of policies, standards and controls form the Enbridge Cyber Controls Framework and the Cyber Security Program and associated Cyber Security Scorecard provide tactics, plans and measurement to reinforce the controls needed to keep risk within acceptable tolerance. This program applies to information and operational technology including Industrial Control Systems.

Concerns with OEB Framework Proposal

Enbridge has developed and implemented a robust, risk-based cyber security control framework to address cyber security unique to all Enbridge businesses and has in place a continuous improvement process to address issues as they are identified and arise over time. EGD submits that application of the Framework to gas distributors, if the Board had authority and were to pursue that course, would not serve the purpose of improving Enbridge's existing cyber security systems. In fact, following the Framework for EGD would be a costly duplication of effort, with no foreseeable value or reduction of risk to Enbridge. Where the Framework deviates from Enbridge standards, EGD may be required to maintain two frameworks that may be conflicting or interpreted in different ways. This would not be workable or efficient. The Staff Report and Framework are also not specific to Enbridge. In Enbridge's experience, it is necessary for cyber security systems to be customized and specific to the applicable businesses in accordance with industry guidelines that are less prescriptive and flexible in their application.

For instance, the Framework uses the C2M2 methodology, which is predominantly process-maturity based, to measure compliance. The Enbridge cyber security control framework is aligned with the NIST Framework which states "Successful implementation of the Framework is based upon achievement of the outcomes…" However, a mature process does not guarantee an effective control. The Enbridge cyber security control framework is designed to measure control effectiveness; it defines specific control metrics to manage cyber security threats unique to Enbridge within the

agreed risk tolerance. While process maturity is an important factor, it is not a comprehensive measure of effectiveness. The Enbridge framework recognizes and addresses this limitation.

Enbridge is currently a member of several well-established information sharing forums such as, Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC), Canadian Gas Association (CGA), Interstate Gas Association of America (INGAA), Canadian Cyber Incident Response Centre (CCIRC) and EGD receives the benefit of Enbridge's participation in these forums. EGD may not provide or receive incremental benefits from participation in the proposed OEB Cyber Security Information Sharing Forum (CSIF) given the main focus is on the Smart Grid and Enbridge already has a mature and robust cyber security framework in place. EGD therefore submits that participation in the CSIF should be left to EGD's discretion. However, EGD remains committed to maintaining robust cyber security systems and welcomes opportunities for effective industry collaboration and education.

EGD is also concerned about the Framework's proposed centralization and detailed reporting of cyber security compliance measures with the OEB. The consulting team (AESI) suggests that a Centralized Compliance Authority (CCA) could be established as a sector-created and managed entity or a separate division within OEB. AESI has recommended in the implementation plan that the self-assessment questionnaire results be managed by the CCA. Typically, these questionnaires contain highly sensitive information that must be protected with extra care and attention. The collection and aggregation of this data from multiple organizations data would be a prime target for cyber criminals and espionage. EGD questions the need for the OEB to act as a central agency for collection of such proprietary and sensitive information.

Conclusion

As requested and required by the Board to support EGD's rates and other regulatory applications, EGD does and will continue to provide cyber security system information to the Board. EGD will continue to follow and operate pursuant to strong Enbridge cyber security standards in accordance with the NIST and other standards noted above. EGD is also interested in participating in future Board cyber security consultatives and working groups in order to share its experiences with and learn from experiences of other OEB regulated entities. In particular, EGD would welcome an in-depth discussion with Board Staff and other gas distributors about the similarities and differences between the gas distributor cyber security systems and the Staff Report and Framework that focus on the Smart Grid and electricity distributors.

The OEB has not provided a clear indication that it intends to mandate the Staff Report and Framework for gas distributors, as would be required by the OEB Act for any rule-making. For the reasons set out above, EGD does not support mandatory application of

the Staff Report and Framework to the gas distributors as necessary or appropriate and we welcome further discussions about gas distributors' existing cyber security systems.

Yours truly,

(Original Signed)

Tania Persad
Senior Legal Counsel