CANADIAN GAS ASSOCIATION
ASSOCIATION CANADIENNE DU GAZ

Sponsor of Ottawa 2017

July 17, 2017

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

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

Dear Ms. Walli:

The Canadian Gas Association (CGA) would like to thank the Ontario Energy Board (OEB) for the opportunity to provide comment on cybersecurity impacts on Ontario's critical energy systems and the privacy of personal information of Ontario energy consumers. CGA is the voice of Canada's natural gas distribution industry. Our members deliver natural gas to over 7 million customers nationally. Our Ontario utility companies - Union Gas, Enbridge Gas Distribution, and Utilities Kingston - deliver natural gas to over 3.5 million Ontario customers. Each customer is a home, a business or an industrial facility.

CGA's Cybersecurity program

The CGA has a cybersecurity strategy which enables technical and strategic information and intelligence sharing and a mechanism for identifying and carrying out initiatives that improve the effectiveness of our members' cybersecurity programs.

Our Cybersecurity Task Force, overseen by a strategic CEO-level steering committee, meets regularly to share information and has developed industry guidance for the security of industrial control systems. This guidance is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The CGA is an affiliate member of the Canadian Cyber Threat Exchange and has recently brought our entire membership into the Downstream Natural Gas Information Sharing and Analysis Centre (DNG ISAC), an ISAC administered by the American Gas Association (AGA) which partners with the Electricity ISAC. The DNG ISAC recently established an MOU with the Canadian Cyber Incident Response Centre (CCIRC) and is working to establish one with the RCMP creating an important Canadian information sharing network.

We are also in the process of establishing an agreement with Communications Security Establishment Canada, and we actively engage on cybersecurity with strategic partners such as the Canadian Electricity Association, AGA, and others.

Towards effective cybersecurity

As Canadian regulators consider their role in cybersecurity and begin to take action, they should do so understanding what has worked and what has not worked in other jurisdictions. Cybersecurity is a dynamic, complex goal to achieve, and there is a perennial risk that a compliance-based approach can

present obstacles to efforts to mitigate/reduce threats, thereby exposing critical infrastructure to unnecessary risk.

The partnership model that exists in the U.S. between the Department of Transportation and the American natural gas delivery industry is an effective model that we encourage Canadian regulators to consider, as it supports a dynamic, risk-based approach for cybersecurity and thereby enables effective protection of natural gas delivery systems.

While CGA does support alignment with the NIST and C2M2 and we believe there is merit in the maturity model approach, even the most mature cybersecurity program does not equate to the most effective one. Consideration should also be given to alignment with other important industry standards such as COBIT, PCI, and ANSI.

Summary and recommendations
CGA and its members request that the OEB give particular thought to the following points:

- We recommend a more substantial consultation with natural gas stakeholders, perhaps via the CGA Cybersecurity Task Force, similar to what took place via the Independent Electricity System Operator with electric stakeholders.
- It can never be understated that compliance is not equal to effective security, therefore we recommend the OEB consider more of a partnership/voluntary model for its regulation of cybersecurity.
- We recommend the *adoption* of standards (e.g. NIST Cybersecurity Framework) as opposed to their *adaptation*. A multiplication of frameworks across jurisdictions will continually erode the value of national and international cybersecurity partnerships.
- The OEB proposed approach to self-assessments, managed by the CCA, creates a potential target for cybercriminals/cyberespionage as this information would contain highly sensitive information from multiple organizations.
- In its 2013 "Supplemental Grid Report", the OEB indicated that the "Board will not develop its own set of cybersecurity and privacy standards, but instead, will require regulated utilities to provide evidence of meeting appropriate cyber-security and privacy standards." We support this approach over the establishment of new frameworks and other jurisdiction-specific requirements.

Once again, we thank you for the opportunity to provide our views on this important issue.

Respectfully,

Timothy M. Egan
President & Chief Executive Officer
Canadian Gas Association