ENERGY+ INC.
1500 Bishop Street, P.O. Box 1060, Cambridge, ON N1R 5X6 • Telephone 519-621-3530 • Fax 519-621-7420

July 14, 2017

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

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

Energy+ Inc. (E+) is an electricity distribution company, providing electricity to 65,000 residential, small, medium and large scale commercial customers in the City of Cambridge, Township of North Dumfries and the County of Brant.

E+ has reviewed the June 1, 2017 Staff Report to the Board On a Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors and the White Paper Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets, (together being referenced as the Framework). We appreciate having insight on the coming regulation and the opportunity to provide comments for consideration.

Comments for the OEB to Consider

1) ***Regulatory Requirements and Reporting***

Confidentiality

Reporting of a LDC's cyber security posture inherently adds risk. As recognized and acknowledged by the OEB facilitators of the OEB's Cyber Security Working Group, all LDC submissions to the OEB must be held confidential with limited information made publicly available. As well, LDCs expect that the OEB will enforce this when requests arise from interveners and third parties. Making known LDC's security posture will only put the LDC, as well as the provincial electrical grid, at risk of compromise and misuse. Hence, it is important to ensure that any reported cybersecurity information remains Highly Confidential.

Reporting

LDCs are currently expected to include cyber security planning and forecasts in the Distribution System Plan. This is re-iterated in the Cybersecurity Framework. E+ agrees that planning and ensuring compliance is necessary as it demonstrates due diligence, good governance and risk mitigation with respect to asset management, and capital expenditure control. Capital expenditures for cyber security may not meet an LDC's materiality threshold. However, if these expenditures are of a material nature, the specific details, vendors and cost of the plan, etc., should not be included in the DSP.

Relevance with respect to the constant changing cyber security environment is also important. The DSP covers a five-year period, throughout which, the cyber landscape will change significantly. During the development of the Framework, participating LDCs were told to expect that the requirements will continuously evolve as the adjustment to this new Cybersecurity Framework unfolds. The programs and associated costs will be adjusted according to the ongoing risks and needs of the LDC as required. Cyber security is an issue that lives in nanoseconds and not the minutes, hours, weeks, months and years that other components of the DSP do and as such, this is not an apples-to-apples comparison nor timeframe that allows for comparison to electrical grid components as captured in the DSP.

Given that the DSP is a publicly available document, it is not confidential. The overall cyber security self-assessment level and the development of annual plans should be reported as a separate confidential filing or included in the annual Reporting and Record Keeping Requirements, as information filed in this manner is held confidential and only disclosed in aggregate, is recommended for reporting purposes.

2) Additional Implementation Tools and Guidance Required

Subjectivity

The Self Assessment Questionnaire (SAQ) is subjective, leading to varied interpretations and differing responses. The Framework suggests that in the first stage of the regulation, there is no provision for an external audit, only a self-attestation. As such, there will be discrepancies among the resulting requirements and implemented controls for entities with similar cyber security risk postures.

Will there be direction forthcoming or a way to identify minimum requirements?

ENERGY+ INC.
1500 Bishop Street, P.O. Box 1060, Cambridge, ON N1R 5X6 • Telephone 519-621-3530 • Fax 519-621-7420

Cost Recovery

The results of the RPT and SAQ leads any LDC to a great number of new initiatives. Undertaking the risk assessments, establishing new cyber security objectives and plans will not only take considerable effort and realignment of internal resources, but there will be costs associated with becoming compliant as defined in the Framework. As such, E+ foresees that there may be additional cost to become and maintain compliance, regardless of the security controls that our organization already has in place.

Recognizing that these new expenses will be staff time, additional IT and OT related expenditures, as well as contracting third party service providers and / or auditors, the majority of these expenses would be deemed Operational Expense versus Capital Expense.

Furthermore, these expenses are not one-time costs. Maintaining a strong cyber security posture in an environment that is ever changing, with a regulation that will incrementally adjust and expand in scope, will require on-going administration and new activities.

Will there be a standardized deferral account for all LDCs to use until their next Cost of Service? The ability to track and recover these additional / incremental costs is consistent with OEB's practices when introducing new initiatives. Given that deferral accounts are not held confidential, their use would put LDC cybersecurity plans at risk.

What has the OEB considered for cost recovery on cyber security expenditures and the need to keep this reporting highly secure? Will the LDCs have input into that process?

Return on Investment

Given the additional expenses, how will the OEB assess an acceptable level of financial burden to meet the level of risk to a LDC? Will there be a metric that compares the quality of the cyber security controls required, relative to the cost to implement them (i.e. a return on investment from a quality of mitigation perspective)?

ENERGY+ INC.
1500 Bishop Street, P.O. Box 1060, Cambridge, ON N1R 5X6 • Telephone 519-621-3530 • Fax 519-621-7420

3) Other Aspects to be Incorporated

Residual Risk Score

Has consideration been given to adding a residual risk score to the SAQ? The individual LDC results of the RPT will be static, very little will change the risk level over time.

A residual risk score from doing the SAQ would not change the corporate risk score as developed from the RPT, but wold demonstrate the level of risk given the controls implemented by the LDC. Subsequently, a residual risk score built into the SAQ would assist LDCs in understanding their level residual risk upon completion of the SAQ. Essentially, the residual risk score will help the LDC to identify those areas where there are gaps between their current risk posture and that put forth in the SAQ. Finally, this SAQ residual risk score would become a means / method on which an LDC could monitor its' progress on risk management and achieving compliance. It also would serve as a good benchmark for industry comparison.

Cyber Security Information Sharing (CSIF)

The OEB indicates that it will work with the industry to establish a CSIF to increase sector awareness and training. How is the OEB planning to establish the CSIF? Who would be the facilitator for the CSIF? How quickly does the OEB wish to see the CSIF come into existence? Who will be the watchdog over the CSIF?

Thank you for your consideration of Energy+ Inc.'s comments and questions. Feel free to contact Paul J. Martinello, Vice President, Information Technology Services at Energy+ Inc. at pmartinello@energyplus.ca, 519-621-8405 ext. 2240, or myself, for any follow-up.

Sincerely,

Ian Miles
President & CEO
Energy+ Inc.
1500 Bishop St. P.O. Box 1060
Cambridge, ON N1R 5X6
Direct: 519-621-8405, Ext. 2355
Phone: 519-621-3530
imiles@energyplus.ca