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

July 14, 2017

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

Utilities Standards Forum (USF) is a forum of Ontario electricity Distributor Members for collaboration and mutual support. Incorporated in 2005, this non-profit has 54 Distributor Members, and operates Forums that support the Engineering, IT, and Regulatory departments. (Distributor Member List can be found in Appendix A).

The GridSmartCity Cooperative's (GSC) mandate is to increase efficiency and customer and shareholder value within our 13 Local Distribution Company (LDC) territories, while benefitting the Ontario electricity sector as a whole. Our member utilities synergize their operations through a cooperative approach to buying and numerous special initiatives. (Member List can be found in Appendix B)

USF and GSC have 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 your consideration.

Collaboration, Training, Templates

USF and GSC have established forums and processes for collaboration in the IT areas of the electricity distributor memberships. The intention of these groups is to utilize these forums for the review of the Framework, and review of the regulatory requirements upon release in Fall 2017. In order to act consistently and cost effectively, the development of common elements and the bulk buying of services will be considered.

As an example, in direct response to the Framework, we will offer the following to the IT teams of our memberships throughout the preparation, planning and implementation phases of compliance regarding this regulation:

- Workshops – facilitated discussions among Members regarding a consistent approach to meet the requirements, collaborative discussions regarding available cyber security services and tools, sharing of implementation experiences
- Training - hiring experts to provide training; i.e. a cyber security / NIST expert explaining the requirements of the Framework, options for and how best to address the requirements in the current environment
- Templates - collectively develop standard template for all potential categories and sub-categories; i.e. assessments, policies, procedures, lists, plans
- Bulk Buying – evaluating service vendors and suppliers collectively, and pursuing volume discounted purchasing agreements

Comments for the OEB to Consider

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.

Reporting

LDCs are currently expected to include cyber security planning and forecasts in the Distribution System Plan (DSP). The Framework reiterates this requirement. The DSP describes the LDCs plans for asset management, and capital expenditures that meet the LDCs materiality threshold. However, the expenses related to cyber security are primarily staff time and contracting third party service providers, which are deemed Operational Expense versus Capital Expense. Accordingly, capital expenditures for cyber security maintenance may not meet the LDCs materiality threshold. Therefore, the specific project plans and cost of the plan, etc, should not be included in the DSP.

Relevance of the changing environment is also important. The DSP covers a five year forecast period, throughout which, the cyber landscape will change significantly. Additionally, the regulatory requirements expect to continuously adjust to this evolving environment. Suitably, a LDCs programs and associated costs will be adjusted according to the ongoing risks and needs as required, potentially rendering medium to long term forecasts inaccurate.

Furthermore, the DSP is not a confidential document, as it is publicly available.

LDCs agree that planning and ensuring compliance is necessary, as it demonstrates due diligence, good governance, and risk mitigation. However, considering all of these points, the DSP is not a suitable mechanism for reporting on cyber security. A separate confidential filing, or inclusion of cyber security in the annual Reporting and Record Keeping Requirements, where by information filed is held confidential and/or only disclosed in aggregate, is recommended for reporting purposes.

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 requirement 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.

Is there a way to identify minimum requirements in a guideline?

Cost Recovery

The results of the Framework assessments, the Risk Profile Tool (RPT) and SAQ, lead any LDC to a great number of new initiatives. Undertaking risk assessments, and establishing new cyber security objectives and plans will take considerable effort and a realignment of internal resources. As such, there may be significant incremental cost to become and maintain compliance, regardless of the security controls a LDC may already have in place. Moreover, 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.

For similar new initiatives, the OEB has previously used standardized deferral accounts for all LDCs to use until their next Cost of Service. However, deferral accounts are not held confidential, so their use would put LDCs at risk.

How does the OEB intend on addressing the need for cost recovery on cyber security expenses, and the need for confidentiality of this reporting?

Return on Investment

Given the additional expenses for compliance to this regulation, 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 mitigation perspective)?

Other Aspects to be Incorporated

Residual Risk Score

The individual LDC results of the RPT will be static and very little will change the risk level over time. Have you considered adding a residual risk score?

A residual risk score would not change the risk level but it would update the risk level based on the controls in place. It would take into account the influence of controls, assessing the likelihood and impact of an incident. Such a score would assist LDCs in understanding the remaining risk by providing a method on which to monitor progress on risk management. It also would be a good metric for industry comparison.

Cyber Security Information Sharing Forum (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? Is there an opportunity for USF to facilitate the CSIF?

USF's membership represents a large portion of Ontario's LDCs and it is poised to draw in appropriate subject matter experts. With a mandate to develop industry standards, share experiences and provide training, USF is well positioned to facilitate the CSIF forum. We are interested in further discussing this opportunity.

Thank you for your consideration of our comments and questions. Feel free to contact Lori Gallaugher, USF Executive Director at lgallaugher@utilitiesstandardsforum.ca, 519-803-3532 with any follow up.

Sincerely,

Keith McAllister

Keith McAllister
President
keith.mcallister@entegrus.com
Utilities Standards Forum
234 Farley Drive
Guelph, Ontario
N1L 1N2

J. Van Ooteghem

Jerry Van Ooteghem
Chair
jvanooteghem@kwhydro.ca
GridsmartCity Cooperative
1340 Brant Street
Burlington, Ontario
L7R 3Z7

GridSmartCity™
renewing energy

USF UTILITIES STANDARDS FORUM

Appendix A

Utilities Standards Forum Distributor Member List as of July 1, 2017

1. Alectra Utilities Corp.
2. Algoma Power Inc.
3. Atikokan Hydro Inc.
4. Bluewater Power Distribution Corp.
5. Burlington Hydro Inc.
6. Canadian Niagara Power Inc.
7. Centre Wellington Hydro Ltd.
8. Chapleau Public Utilities Corp.
9. Collus PowerStream Corp.
10. Cornwall Street Railway Light and Power Company Ltd.
11. E.L.K. Energy Inc.
12. Energy + Inc.
13. Entegrus - Powerlines Inc.
14. EnWin Utilities Ltd.
15. Erie Thames Powerlines Corp.
16. Espanola Regional Hydro Distribution Corp.
17. Essex Powerlines Corp.
18. Festival Hydro Inc.
19. Fort Frances Power Corp.
20. Greater Sudbury Hydro Inc.
21. Grimsby Power Inc.
22. Guelph Hydro Electric System Inc.
23. Hearst Power Distribution Company Ltd.
24. Hydro One Networks Inc.
25. InnPower Corp.
26. Kenora Hydro Electric Corporation Ltd.
27. Kingston Hydro Corp.
28. Kitchener-Wilmot Hydro Inc.
29. Lakefront Utilities Inc.
30. Lakeland Power Distribution Ltd.
31. Midland Power Utility Corp.
32. Milton Hydro Distribution Inc.
33. Newmarket-Tay Power Distribution Ltd.
34. Niagara Peninsula Energy Inc.
35. Niagara-on-the-Lake Hydro Inc.
36. North Bay Hydro Distribution Ltd.
37. Northern Ontario Wires Inc.
38. Oakville Hydro Electricity Distribution Inc.
39. Orangeville Hydro Ltd.
40. Orillia Power Distribution Corp.
41. Oshawa PUC Networks Inc.
42. Ottawa River Power Corp.
43. PUC Distribution Inc.
44. Renfrew Hydro Inc.
45. Sioux Lookout Hydro Inc.
46. Thunder Bay Hydro Electricity Distribution Inc.
47. Tillsonburg Hydro Inc.
48. Toronto Hydro Electric Systems Ltd.
49. Wasaga Distribution Inc.
50. Waterloo North Hydro Inc.
51. Welland Hydro Electric System Corp.
52. Wellington North Power Inc.
53. West Coast Huron Energy Inc.
54. Westario Power Inc.

Appendix B

GridSmartCity Cooperative's Member List as of July 1, 2017

1. Brantford Power Inc.
2. Burlington Hydro Inc.
3. Energy + Inc.
4. Essex Powerlines Corp.
5. Guelph Hydro Electric Systems Inc.
6. Halton Hills Hydro Inc.
7. Kingston Hydro Corp.
8. Kitchener-Wilmot Hydro Inc.
9. Milton Hydro Distribution Inc.
10. Niagara Peninsula Energy Inc.
11. Oakville Hydro Electricity Distribution Inc.
12. Waterloo North Hydro Inc.
13. Welland Hydro Electric System Corp.