ONTARIO ENERGY ASSOCIATION

Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario

EB-2016-0032 Submission

July 13, 2017

To shape our energy future for a stronger Ontario.

Ontario Energy Association

ABOUT

The Ontario Energy Association (OEA) is the credible and trusted voice of the energy sector. We earn our reputation by being an integral and influential part of energy policy development and decision making in Ontario. We represent Ontario's energy leaders that span the full diversity of the energy industry.

OEA takes a grassroots approach to policy development by combining thorough evidence based research with executive interviews and member polling. This unique approach ensures our policies are not only grounded in rigorous research, but represent the views of the majority of our members. This sound policy foundation allows us to advocate directly with government decision makers to tackle issues of strategic importance to our members.

Together, we are working to build a stronger energy future for Ontario.

SUMMARY AND SUBMISSIONS

The Ontario Energy Association (OEA) is pleased to provide this submission on the Ontario Energy Board's (OEB) review of the non-bulk electrical grid and associated business systems in Ontario that could impact the protection of personal information and smart grid reliability (EB-2016-0032).

The OEA commends the OEB's stakeholder consultation process for this initiative on cyber security. OEA members have expressed a high degree of satisfaction with the engagement by the OEB with stakeholders through both the Cyber Security Steering Committee (CSSC) and Cyber Security Working Group (CSWG) in soliciting input and helping to develop the proposed framework.

However, participants at both the CSSC and CSWG raised a number of questions on how some of the proposed elements of the framework (such as governance, certification, audits, reporting and compliance) will actually play out in the long run and what are the definitive roles and responsibilities of various key stakeholders in the framework. Detailed answers to these types of questions are still unknown.

As a result, the OEA is making key submissions in the following areas:

Submission 1: Establishment of the Cyber Security Advisory Committee (CSAC) and Cyber Security Information Forum (CSIF)

The CSAC will be tasked with maintaining an ongoing evolution of the framework and tools as well as the development and proposed mandate of the CSIF.

OEB staff is recommending mandatory participation by utilities in the proposed CSIF group. The purpose of the group is for the industry to share information on cyber incidents, implementation details, cybersecurity awareness, etc. The information shared within the forum will be of high sensitivity. Access and control to the shared information will be a key to the successful implementation of the forum.

The CSIF is intended to be a forum for sector-sharing of data and information in order to improve the efficacy of and evolve the framework. The recommendation of the CSWG is that information shared in the forum would be anonymous. However, there may be a need to strike some balance in order for the forum to be an effective tool to help everyone evolve the project. Complete anonymity may potentially cause roadblocks that may hinder the evolution of effective cyber security in the Ontario electricity industry.

Based on these submissions, the OEA believes that the OEB should address the following questions:

- What platform will the CSIF use to communicate and store shared information? Will it be an existing platform such as the Canadian Cyber Threat Exchange (CCTX) or will one be purposely developed for the industry?
- How will it be ensured that sensitive information does not leave the CSIF forum?
- With all distributors actively involved in the CSIF (a mandatory requirement), would the certification status of each distributor be available to all distributors?

Submission 2: Audits and Reporting

The AESI White Paper (pp. 60-62) refers to and describes the establishment of a Centralized Compliance Authority (CCA). The purpose of the CCA is to collect and summarize information from utilities on their cyber security posture and report to the OEB. It is left unclear if the CCA will be a division within OEB or another sector led establishment. The White Paper states that the CCA: *"could be a sector-created and managed entity or a separate division within OEB"* (p. 60)

OEB staff is suggesting that penetration testing and audits by 3rd parties to be against the OEB Cyber Framework. The audit results are to be provided to CCA. Again, the concern is that highly sensitive information will be leaving energy utilities. It is unclear how this information will be guarded and who will own it. The only reference made in the White Paper is to using a Governance, Risk management and Compliance (GRC) tool.

In determining the risk profile, both subjective and objective approaches are mentioned in the OEB staff report. The issue of cyber security would seem to require an objective approach. More clarity around the meaning of a subjective approach would be helpful.

Based on these submissions, the OEA believes that the OEB should address the following questions:

- Will the CCA be a division within the OEB or another sector led establishment?
- How will it be ensured that sensitive information provided to the CCA will be secure?
- Will the CCA outlined by the AESI whitepaper play a role in auditing?
- What is meant by the "subjective approach" to determining risk profile?
- Will 3rd-party service providers and other entities (including large customers) that interface with utility systems also be subject to audit and/or certification, or will each distributor be ultimately responsible for securing each access point?
- Under Third-Party Independent Validation, the framework provides distributors a mechanism for 3rd-party validation/reporting/auditing using "accredited" organisations:

- What would these accreditations be, and how would consistency in auditing be ensured?
- Could these entities be certified by the distributors to ensure that any 3rd-party auditing organization is aware of the framework, thereby encouraging consistency of audits?

Submission 3: Compliance

OEB staff is proposing that the cyber security framework be implemented in a phased approach.

According to the White Paper, during "Stage 1" an LDC CEO should be providing "Management Attestation" on framework compliance (Compliant, Non-Compliant).

During "Stage 2" a more rigorous approach will be adopted, where the CCA will be conducting testing of:

- Self-assessments
- Desktop audits
- On-site tests, by CCA or accredited independent 3rd party

According to the White Paper (p. 61) the desktop audit:

> "…would require the LDC to provide specific information to allow for a more detailed compliance review […] This may potentially include such as:
>
> - Review policies and procedures …
> - Review any significant changes to hardware/software/etc. and related resources (e.g. staffing, funding, etc.) …
> - Examine the preparation of the annual business plan and technology strategy to ensure:
>   - appropriate allocation of resources;
>   - alignment on strategy across the LDC regarding cybersecurity and general security posture…"

The OEA submits that it is unclear what "compliance" means, how it can be achieved by a utility, and what the consequences of non-compliance will be. Typically, compliance would be achieved through a combination of satisfying all the framework requirements (or a subset of core requirements) and an associated maturity level. However, it is not specified at what maturity level a utility will be considered compliant. Also, it is unclear how much time utilities will have to achieve full compliance with the framework. This could be a multi-year project for a utility that will

result in increased costs for monitoring and other security aspects to achieve compliance.

Based on these submissions, the OEA believes that the OEB should address the following questions:

- What will the compliance structure be for the new framework and how will it be enforced?
- How will a merger/acquisition impact compliance? Will there be a transition period to allow a merged entity to develop a consolidated framework?

energyontario.ca

CONTACT

121 Richmond Street West
Suite 202
Toronto, Ontario M5H 2K1
416.961.2339
oea@energyontario.ca
@energyontario
energyontario.ca

Ontario Energy Association

Let's unravel complex energy challenges, together.