Meeting Summary

OEB Smart Grid Advisory Committee

Meeting Date: October 22, 2013 **Time:** 9:30 am – 3:45 pm

Location: OEB Offices, 2300 Yonge Street

The Meeting Summary provides a high level review of the presentations and discussions at the Smart Grid Advisory Committee. The summary identifies key issues that arise and any conclusions or recommendations by the Committee. It will not attribute comments to any individual organization besides presenters. Agendas, presentations and meeting summaries will be available on the OEB's website under Smart Grid Advisory Committee.

Meeting Agenda

1. Introduction
2. Cyber-security (continued from last meeting)
3. Disseminating Information About Grid Modernization
4. Future Committee Meetings

1. Introduction

- Welcome and introductory remarks; review of meeting agenda
- The main objective of the Committee is to develop advice and recommendations for consideration by the Board
- Agenda for the meeting:
    - Identify next steps for how the Committee will proceed with formulating advice to the Board regarding cyber-security
    - Discuss the best ways to facilitate sharing of information about grid modernization among distributors.

2. Cyber Security

The Board's Supplemental Report on Smart Grid indicated the following:

- Cyber-security has always been important to the Board
    - As smart grid technologies and processes are implemented must ensure that cyber-security measures are upgraded accordingly
- Regulated entities expected to provide evidence of appropriate cyber-security measures
    - e.g. provide third party audit confirming adherence to a given standard, model, best practices, framework, etc.

2.1 – Cyber Security (Presentation by IESO)

- Presentation is available on the website
- Comment and Questions from the Committee
    - It is important to encourage a focus on security rather than on compliance.
    - To that end, LDCs will need access to information about existing threats and how to protect their systems. Need some way to facilitate information dissemination without compromising security.

2.2 – Next Steps to address Cyber-security (Discussion)

- What can we do to raise awareness and understanding of best practices / principles among distributors? And what can we do to promote responsible sharing of information among the sector?
    - the Canadian Cyber Incident Response Centre is a great resource for LDCs
- Is there a further role for the OEB? Further guidance needed?
    - Difference between standards and best practices. No point in OEB mandating standards unless monitoring and compliance goes with it. Whereas providing guidelines on best practice allows more flexibility.

- Need end to end security but, within that, also need to look at security in segments and judge risk level associated with each:
    - e.g. customer interface has different risks and requirements than machine to machine interfaces within the network. Additionally, Dx to Tx interface is critical for Hydro One but probably less so for other LDCs
    - Three segments identified (risk and requirements different for each):
        - Public domain (customer data, HAN / AMI interface) – requires high security;
        - Intra-network – need a reasonable amount of security for enterprise systems;
        - Intra-network – need greater protection for critical infrastructure.
- When developing best practices should consider including user access / design principles.
- Need to also think about not linearly scaling up but best practices that allow reasonable expenditures for LDCs of varying size and scope.
    - Cyber-security framework / procedure / capabilities is risk driven, each LDC needs to know how to right size investment based on risk. Perhaps the OEB could provide some guidance about how to make decisions about the right level of investment based on the risks associated with your enterprise?
- Is there a benefit to doing some information gathering from distributors about current status to get an idea of current state of security?
    - There are a number of maturity models that could be used as a basis for a questionnaire – where are you on the maturity model? Not good or bad, just where are you? Doesn't require a lot of dating mining to respond.
    - Questionnaire could be industry wide – similar questionnaire (maturity model) could be adapted for all market participants.
    - Would show where entities are and where they need to go.
    - Exercise will help LDCs understand where they are (against themselves and their peers). Also gives the Board a starting point for information
    - Part of the objective is to have a common understanding of where we are and what are we doing – using questionnaire may have the effect of spreading common language so we all understand each other.
    - Should not widely share results but a core group could be struck to evaluate the results.
    - Could there be a role for the EDA in collecting / disseminating this type of information?
- Need to understand the threat / risk landscape – along with an understanding of where utilities are in the maturity model – together these will help us draft a best practices/ principles document.

- Working group to be established to take an existing open, non-proprietary security maturity model questionnaire (e.g. DOE's questionnaire or similar) and adapt it for our purposes.
    - Purpose of questionnaire is to gather information to make decisions about further guidance and also signal LDCs to start thinking more about cyber-security.
    - To be determined if questionnaire will come from the Board or the SGAC

3. Disseminating Information about Grid Modernization

3.1 – Smart Grid Plan (Presentation by Hydro One)

- Presentation is available on the website

3.2 – Disseminating Information to Assist LDCs (Discussion)

- How do we support dissemination of information among LDCs? E.g. information about:
    - results of pilot and demonstration projects that inform full roll-out decisions (why this did / didn't work for my utility; can help other utilities decide if it may / may not work form them – recognizing that what works for some may not work for others and vice versa)
    - how a successful business case / strategy was developed.
- Challenges associated with formal or public sharing of this information
    - Open to misinterpretation; information loses value when it is not shared in a forum conducive to discussion (e.g. bulletin, website etc.); vendor / utility confidentiality issues. . . etc.
- Conversely, if dissemination is very informal it can be more effective, but it may not reach everyone that it needs to (e.g. the distributors not at the table)
- Ultimately there is no one methodology – sometimes LDCs will just reach out to each other directly, sometimes information will be shared at forums such as this.
- Beyond the information presented that can be found in the evidence included in Hydro One's rate application, what did people find useful in the presentation that they wouldn't find in the evidence itself?
    - Advice to other distributors – key messages about benefits and measuring them. That was the value added.
    - High level discussion of what are the alternatives and why you went with smart grid option would be helpful to other utilities – highlight that these decisions are utility specific so take from others' experience what makes sense for you.
- As a starting point, what about a list of who's doing what (e.g. which LDCs are doing energy storage, EVs etc.)

    - Online database exists for this. It's free. SG Canada Clearinghouse, drawback is it may not consistently be up to date.
        - Challenge is getting utilities to post information.
- What about a broader gathering of LDCs where presentations such as this occur?
    - "E8" utilities do this quarterly.
        - This ensures there are no big gaps or overlaps among the large distributors in their SG pilots and tests.
    - EDA is looking at this. Utility members should pressure EDA to focus on disseminating this type of information. Should be careful not to let it become too Ontario-centric though. . .
        - However, EDA is very exclusionary to customers. May need an additional forum to capture that dimension.
    - Agreement that EDA is best vehicle for this type of information sharing
        - Would recommend that whatever method the EDA lands on has some mechanism for reporting back to SGAC so that we stay in the loop.
        - Mechanism to share information outside of EDA for example with the grid operator, consumers etc., is an important consideration.
- Should SGAC send out a request to LDCs for their 'smart grid contact' which we can engage with when needed?

4. Closing and Future Meetings

- Working group addressing cyber-security questionnaire to be underway:
    - Terms of Reference to be drafted by Board staff and approved by the Committee
- Next meeting November 26
    - Possible meeting topics:
        - Feedback on status from storage and data access working groups
- Topic for December 17 meeting:
    - Update from distributor members about discussion with E8 on sharing of information (next E8 meeting on December 10).
- Future meeting dates:
    - December 17
    - January 16