Meeting Summary

OEB Smart Grid Advisory Committee

Meeting Date: October 1, 2013 **Time:** 9:30 am – 4:00 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
3. Standards Development
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:
    - Consider how the Committee will proceed with formulating advice to the Board regarding cyber-security including:
        - Identifying main questions for consideration
        - Developing preliminary plan for delivering advice to the Board
    - Discuss the current state of standards development and how the Board might best monitor ongoing developments.

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
- Board doesn't intend to set a standard for cyber-security
- 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 N Dimension)

- Presentation is available on the website
- Comment and Questions from the Committee
    - Is there a 'threshold' that distributors can apply to their assets to help more easily determine which ones are 'critical' and must be protected accordingly?
        - Since there is so much variation among distributors, identifying such a threshold may not be very helpful in promoting the security of the network. The best approach is for each distributor to evaluate their assets and determine whether they are critical.

2.2 – What are the current practices with respect to cyber-security in Ontario? (Discussion)

- Coordination
    - LDCs are already collaborating on securing (and testing the security of) their AMI networks; this should be encouraged and can also occur in

relation to SCADA systems and other utility communications and data systems.
    - Collaboration is cost-effective and promotes good security
    - Collaboration has also increased the influence Ontario LDCs have over vendors (i.e. to encourage vendors to provide support needed and or improve 'built in' security measures)
- Reporting and information sharing
    - Apart from internal reporting within LDCs, not a lot of reporting on cyber-security 'events', threats, or practices
    - It is important to share information among the industry to promote cooperation and a common understanding of current practices and threats
        - However, such information must also be safeguarded from broader availability
        - Confidentiality is important because the more information available about a security framework the more vulnerable it will be
- Customer interests
    - Security measures should provide protection without preventing, or creating unreasonable barriers to, data and services that customers might desire.
    - Customers are likely more concerned with security with respect to privacy rather than system reliability.
    - If / when a security event occurs customers will likely judge LDCs on, did you take reasonable action to prevent this and did you have a plan in place for recover?
        - An outage caused by a cyber-attack will be viewed by the public as more preventable than one caused by a storm for example.

2.3 – Are common standards emerging? (Discussion)

- Standards are in place or under development however they may not be applicable to Ontario's LDCs.
    - E.g. NERC's CIP requirements are likely 'overkill' for distributors because they are focused on protecting the bulk system
- There are pros and cons related to standards in this area.
    - Standards can promote consistency which can help keep costs low.
    - Yet, codifying standards could inadvertently result in codifying a 'weakness' that hackers could take advantage of.
- NIST's cyber-security framework, still under-development, will likely include key elements of a robust, end-to-end security plan (including threat /risk assessment, and recovery plans) it may also reference some standards. Though aimed at bulk

system security, this framework may be scalable for Ontario's LDCs because it will set out good practices and principles rather than a prescriptive approach.

- In the absence of clear standards, there may be value in crafting or referencing a 'best practices' document to help LDCs understand what they should be doing in respect of cyber-security (a somewhat new area for many) and evaluating the services provided by third party security companies.

2.4 – What are the characteristics of a comprehensive and prudent cyber-security program? (Discussion)

- Each LDC will have to identify the assets that are critical to its operations to determine the appropriate level of protection. Critical assets will vary considerably among LDCs so there is no obvious definition or threshold that can be universally applied to identify those assets.
  - Separate focus on inter-system security and intra-system security is encouraged.
- "operationalizing" security will be an important consideration:
  - The culture of organizations will need to incorporate security practices the way that safety is incorporated today (e.g. "baked-in" from the start).
  - Staff training will be important.
- Recovery plans must be in place. Nothing is 100% preventable so LDC's need a plan for how they will react if / when something occurs.

2.5 – Is there a need for further guidance from the Board? How should the Committee monitor cyber-security issues? (Discussion)

- Since cyber-security is a relatively new consideration at the LDC level, some LDCs would appreciate more specific guidance from the Board on what to do (e.g., best practices, or a prescriptive approach that could be adopted voluntarily).
- Other LDCs feel strongly that decisions about cyber-security practices should be left to the LDC and not prescribed by the Board. Third party experts will be retained to help LDCs put security measures in place and the experts will identify the best principles and practices. Like any other investment, the LDC will have to prove the prudence of its cyber-security investments to the Board. Therefore, no further guidance is needed.
- Collaborating with other LDCs has helped some LDCs figure out what they need to do.
- There may be value in requiring or encouraging more reporting / information sharing among industry of cyber-security threats and events.

    - Such data collection would also allow the industry to understand the scope of attacks (both successful and unsuccessful) which could then inform security investment decisions.
- The Committee will revisit this issue, at that time:
    - best principles/practices may be identified to guide distributors;
    - an update may be provided from entities involved in national / international cyber security standards development;

3. Standards Development

3.1 – Smart Grid Interoperability Standards (Presentation by IESO)

- Presentation is available on the website

3.2 – Interoperability Standards (Discussion)

- The pragmatic problem with standards in general is how to pick the right standard at the right time (since Ontario is too small a market to influence which one becomes the standard).
    - The Board has indicated that LDCs should make investments that are 'standards-based' but given the challenges in picking the right standard at the right time, as an industry we may have to accept that sometimes the wrong standard will be picked and assets will be stranded.
        - At the same time, there is no need to 'strand' assets earlier than is absolutely necessary by forcing the adoption of a standard within a short time-period.
- The Committee will revisit this issue from time to time in order to stay up to date on standards development and identify any advice the Committee might provide to the Board on this issue.

4. Closing and Future Meetings

- Working groups addressing issues related to storage and data access to be underway this month:
    - Terms of Reference for each of the working groups will be revised based on comments from the Committee
- Next meeting October 22
    - Committee suggested revisiting cyber-security
- Future meeting dates:
    - November 26
    - December 17
    - January 16