Ontario Energy Board
Commission de l'énergie de l'Ontario

Smart Grid Advisory Committee

Cyber Security & Standards

Board Staff Presentation

October 1, 2013

Agenda

9:30 - 9:45	Welcome; Introductions	Board staff
9:45 - 10:15	Presentation by N-Dimension	Doug Westland
10:15 - 10:45	Cyber-Security Discussion	All
10:45 - 11:00	*Break*	
11:00 - 12:00	Cyber-Security Discussion (cont.)	All
12:00 - 12:45	*Lunch (provided)*	
12:45 - 1:20	Cyber-Security Discussion (cont.)	All
1:20 - 1:50	Presentation by IESO	Edward Arlitt
1:50 - 2:45	Standards Discussion	All
2:45 - 3:00	*Break*	
3:00 - 3:30	Standards Discussion (cont.)	All
3:30 - 3:45	Working Groups	All
3:45 - 4:00	Future Meetings & Other Business	All
4:00	Adjourn	

Today's Objective

- Determine how the Committee will proceed with formulating advice to the Board regarding cyber-security
  - Scoping discussion
  - Identify main questions for consideration
  - Develop preliminary plan for delivering advice to the Board
- Initial Discussion on standards development

Board's Supplemental Report on Smart Grid

- 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.

Issues to keep in mind. . .

- Cyber-security practises in Ontario will be influenced strongly by standards and practices from Canadian federal government, the United States (e.g., US Departments of Energy and Homeland Security), and elsewhere (e.g., EU)

- Needs will vary among transmitters and distributors:
  - Transmitters held to higher standard to promote North American grid security
  - Cyber-security needs & practices will vary among distributors based on varying degrees of risk (e.g. degree of network automation and/or information flow)

- Cost is an issue:
  - Level of cyber-security must be commensurate to level of risk
  - 100%, absolute security is unattainable

- Recovery plans: prevention is important, but also need to be able to achieve rapid and efficient system restoration in the event of a successful cyber-attack

Preliminary Questions

- What are the current practices with respect to cyber-security in Ontario…
  - What are the risks and vulnerabilities to the power system and information infrastructure?
  - Cyber-security programs and procedures in place (including recovery and adequate human resources)?
  - Reliance on mechanisms ‘built’ in by vendors vs. custom cyber-security measures?
  - Reporting and statistics of cyber-security events?
  - Frequency of audits?
  - Degree of coordination with distributors-transmitters-generators-service providers?

Preliminary Questions

- Are common standards emerging?
  - What standards are being utilized in Ontario? (e.g., NERC & NIST)
  - What part of the electricity network are cyber-security standards needed most? (e.g., distribution, transmission, bulk generation)
  - Who is (or should) be leading the way? (e.g., provincial, federal, United States, industry)
  - How can (and should) cyber-security standards be integrated with interoperability standards?
  - What future standards are under development and/or discussion?

Preliminary Questions

- What are the characteristics of a comprehensive and prudent cyber-security program?
- What should trigger Board action on cyber-security?
- Is there a need for further guidance from the Board?
  - To endorse specific standards, models, best practices, etc.?
  - To ensure ‘response procedures’ are in place for all network operators?
  - To require utilities have a cyber-security strategy & plan, conduct risk assessments, reporting of security events/breaches?
  - To give direction on frequency of audits?

Preliminary Questions

- What are the main cyber-security issues for Ontario?
- How should cyber-security issues be monitored by the Committee?
- How often should Committee revisit status of cyber-security developments and identify issues?

Supplemental Report: Standards

- The Board does not intend to prescribe interoperability standards (e.g., communication protocols between meters and “behind the meter” technologies), but expects interoperability
- The Board will take action (e.g., prescribing standards for data access and presentment) in the event that customer friendly data access mechanisms do not emerge

Preliminary Questions

- What components of the grid would standardization be of most value?
  - Interoperability?
- What should trigger Board action on standards?
- How should standards-related issues be monitored by the Committee?
- How often should Committee revisit the status of standards developments and identify issues?

Data Access & Storage Working Groups

- Draft terms of reference have been provided
- Board staff will arrange meetings (in-person or conference call) and provide background materials, assist with research
- Working Group members are responsible for developing recommendations to bring back to Committee

Future Meetings & Other Business

- Future 2013/2014 Meetings
  - October 22
  - November 26
  - December 17
  - January 16

- Any other business?