Cyber-security Questionnaire for Ontario Electricity Distributors

Update:

We had a relatively poor response to the Cyber-security questionnaire sent out in July, 2014. Some distributors expressed concern about the security of the response over e-mail and the possibility that the information might be used in Board proceedings other than the Smart Grid Advisory Committee. To try to alleviate those concerns, Board staff has altered the Questionnaire to remove the distributor name. Instead the questionnaire asks three questions that will allow Board staff to aggregate responses to look for trends by region and size. In addition, Board staff is now suggesting that the responses be filed through the web portal.

Please file your completed questionnaire by February 13, 2015.

Distributors who have already filed a response do NOT have to do so again.

Preamble:

The electricity sector, like other critical infrastructure sectors, has been and will continue to be subject to cyber-security threats and incidents. These risks require organizations to develop and support robust cyber security and cyber-incident response programs to protect themselves from threats to their critical business operations.

Increasingly, the Ontario electricity sector is being required to address cyber-security threats. This escalation obliges organizations to seek out solutions that go beyond traditional compliance requirements to protect privacy, information, and operations.

This document poses questions to guide executive-level discussions about cyber-security risk management for electricity distributors in Ontario, along with cyber risk management concepts. The purpose of this questionnaire is to engage key decision makers on cyber-security issues and risk, and provide the Smart Grid Advisory Committee with information regarding the current state of awareness among Ontario's electricity distributors.

Individual questionnaire responses will be kept confidential by Board staff and will not be published or posted online. Non-identified information will be shared with members of the Smart Grid Advisory Committee and other Board staff in order to inform discussion regarding cyber-security issues and develop any potential policy options or further consultation with electricity distributors.

Please file your completed questionnaire by February 13, 2015. The accompanying template is to aid your response.

Distributors who have already filed a response do NOT have to do so again.

To help us, Distributors must use the naming convention and document submission standard outline by the Board, starting with **CONFIDENTIAL** at the beginning of your document name, and quote the file number **EB-2013-0294. i.e. CONFIDENTIAL_EB-2013-0294 _CyberSecurity_yymmdd_hhmm.xlsx**

All filings to the Board must be made electronically in a searchable / unrestricted MS Excel format through the Board's web portal at https://www.pes.ontarioenergyboard.ca/eservice/. If the web portal is not available, parties may email their documents to boardsec@ontarioenergyboard.ca.

Appendix A:

The attached excel spreadsheet is what is expected to be completed and submitted.

Questions:

Part 1 – We are asking some questions that will allow us to categorize the distributors and look for trends without knowing exactly who they are.

1) Where are you located?
    a. Select your Region as defined by EB-2011-0043 from the options provided.
    For further information on the regions, see http://www.hydroone.com/regionalplanning/Pages/home.aspx.
    If your distribution company is in multiple regions, please select the one that you feel is the most representative.
2) How many residential customers do you serve?
    a. Select the number of residential customers served by your distribution company from the ranges in the drop down menu.
    This could be a current number or for the most recent year for which data is available. The LDC yearbook for 2013 is available on the Board's website, and states the figure for 2013.
3) How big is your system?
    a. Select the average peak load served by your distribution company from the ranges in the drop down menu.
    This could be for the most recent year for which data is available. The LDC yearbook for 2013 is available on the Board's website, and states the number that you said for 2013.

Part 2 – How does your organization deal with Cyber Security?

4) Does your organization have Executive-level accountability for cyber-security? Describe briefly.
    a. If not, at what level of the organization is cyber-security considered? Please describe briefly.

5) Does your company have a cyber-security program or business unit responsible for meeting program objectives?
    a. Does your cyber-security program apply industry standards and best practices? Please describe briefly (e.g., governance, compliance,

employee training and awareness, capital planning, threat risk assessment)?

b. Has your cyber-security program been reviewed by a third-party? How often?

c. How did you address issues identified in the review?

d. What approximate percentage of overall enterprise and operational IT capital and IT operating budget is dedicated to your cyber-security program?

6) Do you use cyber-attack detection and reporting capabilities? Please describe briefly.

a. How many and what types of cyber-incidents do you detect in a normal week?

b. What is your policy for reporting cyber-incident information to management and/or executive leadership?

c. Do you share cyber-incident information with external organizations? Please describe briefly.

d. Does your cyber-security program have a process to actively identify new threats and adjust mitigations accordingly? Please describe briefly.

e. Do you engage with external security organizations to gain insight into new potential threats? Please describe briefly.

7) Do you have a cyber-incident response plan? Please describe briefly.

a. How often is it reviewed and updated?

b. How often is it tested?

c. Is it tested internally or by a third-party?