Ontario Energy
Board
P.O. Box 2319
27th Floor
2300 Yonge Street
Toronto ON M4P 1E4
Telephone: 416- 481-1967
Facsimile: 416- 440-7656
Toll-free: 1-888-632-6273

Commission de l'énergie
de l'Ontario
C.P. 2319
27e étage
2300, rue Yonge
Toronto ON M4P 1E4
Téléphone: 416- 481-1967
Télécopieur: 416- 440-7656
Numéro sans frais: 1-888-632-6273

Ontario

BY EMAIL AND WEB POSTING

March 15, 2018

NOTICE OF AMENDMENTS TO CODES

AMENDMENTS TO THE TRANSMISSION SYSTEM CODE AND THE DISTRIBUTION SYSTEM CODE TO ADDRESS CYBER SECURITY FOR ELECTRICITY TRANSMITTERS AND DISTRIBUTORS

OEB FILE NO.: EB-2016-0032

To: All Licensed Electricity Distributors
All Licensed Electricity Transmitters
All Participants in Consultation Process EB-2016-0032
All Other Interested Parties

The Ontario Energy Board (OEB) has today issued amendments to the Transmission System Code (TSC) and the Distribution System Code (DSC), as described in Section C, pursuant to section 70.2 of the *Ontario Energy Board Act, 1998* (Act).

A. Background

On December 20, 2017, the Board issued a Notice of Proposal to Amend a Code (December Notice), in which the Board proposed a number of amendments to the DSC and TSC (Proposed Amendments), in order to implement the policy objectives set out in the June 1, 2017 Staff Report to the Board.

The Proposed Amendments would if adopted, establish regulatory requirements for licensed transmitters and distributors to provide the OEB with information on the actions they are taking relative to their cyber security risks.

As indicated in the December Notice, the Proposed Amendments rely on the establishment and ongoing evolution of the industry-developed Ontario Cyber Security

Framework (Framework)[1] developed during the OEB`s consultation process, as the common basis for assessing and reporting cyber security capability to the OEB.

The OEB received written comments on the December Notice from four (4) stakeholders: the Coalition of Large Distributors (CLD), the Electricity Distributors Association (EDA), the Utilities Standards Forum (USF) and the GridSmartCity Cooperative (GSC).

B. Adoption of the December Proposed Amendments with Revisions

The comments received from stakeholders generally supported the proposals in the December Notice, including the proposed requirements to report on the status of cyber security readiness and ability, although some stakeholders suggested the need for certain clarifications. Stakeholder groups recognized the extensive consultation work undertaken by the OEB to develop the proposed regulatory requirements as appropriate and worthwhile first steps to support implementation efforts.

The OEB has considered the comments received in response to the Proposed Amendments and determined that no material changes are required. In light of the comments, however, the OEB has made two (2) minor revisions to the Proposed Amendments. The OEB is adopting the Proposed Amendments with those revisions (Final Amendments).

The Final Amendments to the TSC and DSC, as adopted by the OEB, are set out in Attachments A and B. Attachment C to this Notice sets out for information purposes only a comparison version showing the revisions made to the Proposed Amendments as reflected in the Final Amendments.

Revisions to the December Proposed Code Amendments

Definitions of Cyber Security (TSC section 3B.2.1, DSC section 1.2)

In their comments on the December Notice, stakeholders suggested modifications to the definition of “Cyber Security”. The EDA and CLD[2] submitted that the definition was “too broad”. Stakeholders recommended adoption of the National Institute of Standards and Technology (NIST)[3] definition and a narrowing the scope of physical security issues as they related to cyber security protection. The OEB has considered the comments received and determined it appropriate to revise the “Cyber Security” definition to specify that it includes both electronic and physical security *as they relate to cyber*

[1] OEB – Dec 2017 – Ontario Cyber Security Framework
[2] Electric Distributors Association (EDA) and Coalition of Large Distributors (CLD).
[3] NIST

security in both the TSC and DSC.

Stakeholder Comments on Reporting and Self-Certification

The Amendments establish regulatory requirements for all licensed transmitters and distributors to provide the OEB with information on the actions they are taking relative to their cyber security risks.

In general, stakeholder comments were supportive of the proposed reporting requirements. In the coming months, the OEB intends to work with sector stakeholders to develop the self-certification requirements to meet the OEB's requirements and stakeholder concerns.

During the consultation, some stakeholders suggested postponing implementation of the reporting and compliance requirements, as the Framework had not been fully tested in order to calibrate the assessment approach. In response, the Framework was revised and tested further. The OEB understands that the industry developed Framework will need to evolve based on experience.

The OEB is of the view that cyber security is too critical, given the evolving technology in the sector, to delay implementation of reporting. An interim (3 month) progress report is critical to ensure that all have reviewed and understood the Framework, and are taking steps to assess their cyber security readiness. The annual cyber security assessment provides the OEB with information from licensed transmitters and distributors about their current maturity relative to the best practice objectives established in the Framework.

In their submissions, stakeholders also sought clarity with respect to the role the OEB would play in the collection of self-certification details and compliance auditing. In the December Notice, the OEB advised stakeholders that it would use self-certification to understand the cyber security maturity of licensed transmitters and distributors and this might result in follow-up[4] activities. Follow-up activities may be carried out in order to clarify responses received. The OEB's audit planning incorporates information and data received by the OEB and will incorporate the cyber security self-certification reports.

Several stakeholders expressed concerns about disclosure of the self-certification status and the storage of confidential information, citing that additional measures and protections be established to keep reporting data safe. Stakeholders also requested the OEB redact information deemed confidential in their public filings.

The OEB acknowledges that cyber security reports received from licensed transmitters and distributors will contain some sensitive information. The OEB acknowledges the

[4] Through OEB's annual Audit and performance assessment program.

sensitive nature of the reports and does not intend to disclose the self-certification status of licensed transmitters and distributors as part of public filings. The OEB will keep the reports as confidential[5] and will segregate them from other records. Access will be limited to individuals within the OEB who require this information as part of their duties and work assignments.

Both the Electricity Distribution and Electricity Transmission licenses contain provisions that require regulated entities to maintain records and provide such information as the OEB may require from time to time. Archival documentation for the self-certification reports will be consistent with the OEB's Mandatory Records Retention Period Policy for Regulated Entities.

The OEB reminds licensed transmitters and distributors that they are responsible for managing their businesses in a manner that achieves their reliability, security and privacy obligations. Cyber security represents one risk amongst several, in licensed entities' enterprise risk management processes.

C. Future Mechanisms for Cyber Security Cooperation

The OEB views the work carried out by the Cyber Security Working Group (CSWG)[6], in developing the Framework as an excellent step towards sector capability and resilience. To sustain momentum, the OEB expects the electricity sector to continue to collaborate in sharing experiences, knowledge, and information in order to improve its overall capability. Information sharing and Framework evolution are two critical elements for the future.

1. Cyber Security Information Sharing Forum (CSIF)

The December Notice identified the importance of information sharing among utilities to support the evolution of their cyber security capability, enhanced risk awareness and the sharing of best practices. Without this collaborative approach, it will be difficult to acquire a universal understanding of global risk and response developments and to be able to self-certify. Moreover, participation in information sharing allows for the demonstration of good utility practices adopted by many licensees to date, including involvement in the IESO's Cyber Security Forum.[7]

The Notice also set out the OEB's view that a centralized approach to the sharing of information would provide the best opportunity to achieve the benefits identified by the

[5] OEB – Oct 2016 – Practice Direction on Confidential Filings
[6] Cyber Security Working Group (CSWG) comprised of licensed electricity distributors, representatives of the Ontario Ministry of Energy, IESO, the Electrical Safety Authority and Natural Gas utilities.
[7] IESO Cyber Security Forum

CSWG. Comments received from industry in response to the December Notice are supportive of an information sharing mechanism and the creation of a CSIF, citing it as "the most cost-effective way" to support awareness of security issues, concerns, and mitigation to improve security at all levels. To attain a robust information sharing approach, stakeholders recommended a central agency offer the service to the sector, noting it could be acted on "within the shortest period" with the leadership of the IESO. The OEB will support efforts by licensed transmitters, distributors, and the IESO to develop an effective means of institutionalizing information sharing so that it achieves the benefits discussed above.

2. Cyber Security Advisory Committee (CSAC)

In response to the December Notice, stakeholders sought clarification from the OEB regarding its proposed establishment of a CSAC as a standing committee to manage the evolution of the Framework. The OEB expects the CSAC to incorporate industry comments into their approach towards evolving the Framework. Stakeholders' feedback suggested that implementation assistance, support, and guidance would enhance the efficacy of the Framework. In the comments, stakeholders expressed the view that as the Framework evolves, based on advances in cyber security it will be critically important to preserve and enhance the collaborative environment that was established.

As stated in the December Notice, the OEB expects the industry to work, through an appropriate forum to evolve the Framework in a collaborative manner and incorporate stakeholder feedback when and if it is felt that it will enhance achieving the licensees' ability to meet their obligations. The ongoing evolution of the Framework will provide a valuable guide to licensed transmitters and distributors to support their cyber security maturation.

The OEB reiterates the importance of establishing a mechanism to manage the Framework. To this end, the OEB will ask the members from the original CSWG to form the initial CSAC. Early steps in developing the CSAC are expected to include establishing: terms of reference, governance, and change management process (Framework change request, modification, and sector approval method) acceptable to the licensed transmitters and distributors.

3. Centralized Compliance Authority (CCA)

The CSWG suggested that the CCA could be a sector-led initiative to share some level of operational detail among peers, in a confidential manner, in order to reach a deeper understanding of sector matters including performance and best practices, etc. In their submissions, stakeholders expressed concerns about the structures, processes, and support mechanisms and expressed a desire for the establishment of a CCA similar to

sector-based Information Sharing and Analysis Centers (ISACs).[8] Stakeholders recommended that industry should play a "prominent role" in establishing the CCA; and sought additional guidance from the OEB. It is OEB's expectation that the sector will consider this approach, and determine if they wish to undertake this as part of the sector maturation.

The OEB expects that the formation of the CSIF, and CSAC, will result in stronger sector capability through collaboration and sharing of experiences and solutions providing a valuable guide to support licensed transmitter and distributor maturation.

D. Other Stakeholder Comments on the Framework

The EDA acknowledged the Framework as a "suitable starting point" to guide licensed distributors in "managing the evolution of their cyber security maturity". Additionally, strong support was expressed by stakeholders for the adoption of the NIST Framework as it is seen to be "flexible, and descriptive" in nature, allowing for different implementation strategies. Stakeholders also expressed support for the use of the Framework and proposed mechanisms, noting that the Framework would "benefit both distributors and transmitters".[9] The USF and GSC[10] submitted that the "risk levels, security controls, and reporting requirements were defined enough to move ahead".

E. Benefits and Costs

The OEB believes the Amendments set out in this Notice will result in benefits that exceed any additional costs and will result in better information about the sector's cyber security readiness and its ability to protect the privacy of consumers' information.

Application of the Framework by licensed transmitters and distributors will provide a method to assess existing capability against industry recommended best practices. The OEB expects this approach to provide a consistent reference point to assess licensed distributors' and transmitters' cyber security risk and capability. Licensed transmitters and distributors will be better informed as they work to incorporate cyber security into the enterprise risk management decision making, and investment planning that will ultimately form part of their business plans and their transmission and distribution system plans (as applicable).

---

[8] ISACs - assist critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. For example, E-ISAC and F-ISAC.
[9] Coalition of Large Distributors (CLD) consists of Hydro One Networks Inc., Alectra Utilities Corporation, Hydro Ottawa Limited, Toronto Hydro-Electric System Limited and Veridian Connections Inc.
[10] Utilities Standards Forum (USF) – represents 53 electricity distributor members and Grid Smart City (GSC) represents 13 local distribution companies.

F. Coming into Force

The Amendments to the TSC and DSC as set out in Attachments A and B to this Notice come into force on March 15, 2018, being on the date published on OEB's website. Licensed transmitters and distributors are required to submit to the OEB their interim cyber security self-assessment reports no later than June 15, 2018. Annual self-certification of cyber security maturity will be required starting on April 30, 2019. Instructions for the completion and filing of the reports[11] will be set out in the OEB's Reporting and Record Keeping Requirements (RRR) and posted on OEB's webpage.

This Notice, including the Amendments to the TSC and DSC, set out in Attachments A and B will be available for public inspection on the OEB's website at www.oeb.ca and at the OEB office during normal business hours. Questions regarding the matters addressed in this letter should be directed to IndustryRelations@oeb.ca, or by phone at 416-314-2455 or 1-877-632-2727 (toll-free within Ontario).

DATED at Toronto, March 15, 2018

ONTARIO ENERGY BOARD

Original signed by

Kirsten Walli
Board Secretary

Attachment A – Amendments to the Transmission System Code
Attachment B – Amendments to the Distribution System Code
Attachment C – Comparison Version of Amendments

[11] Annual and interim reports.

Attachment A

Notice of Amendments to the Transmission System Code

March 15, 2018

EB-2016-0032

Amendments to the Transmission System Code

Section 3B of the Transmission System Code is amended by adding new sections as follows:

3B Reliability and Integrity of Transmission System

3B.2 Cyber Security

3B.2.1 Definitions

"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access. Cyber security includes electronic security and physical security issues as they relate to cyber security protection.

"Cyber Security Framework" means the Ontario Cyber Security Framework that was issued December 20, 2017, or the current version of the document

3B.2.2 Reporting

3B.2.2.1

A transmitter shall report to the Board on the status of cyber security readiness referencing the Cyber Security Framework at such times and in such a manner as may be directed by the Board.

3B.2.2.2

The Chief Executive Officer of the transmitter shall certify the transmitter's reported cyber security readiness in such form as may be required by the Board.

3B.2.3 Continuing Obligations Regarding Transmission System and Privacy

Nothing in this section 3B.2 shall limit any obligations of a transmitter to maintain the reliability and integrity of its transmission system, and to protect personal information.

Attachment B
Notice of Amendments to the Distribution System Code
March 15, 2018
EB-2016-0032

Amendments to the Distribution System Code

Section 1.2 of the Distribution System Code is amended by adding new definitions as follows:

1.2 **Definitions**

"Cyber Security" means *a* body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access. Cyber security includes electronic security and physical security issues as they relate to cyber security protection.

"Cyber Security Framework" means the Framework Ontario Cyber Security Framework that was issued December 20, 2017, or the current version of the document.

Section 6 of the Distribution System Code is amended by adding new section 6.8 as follows:

6.8. Cyber Security

6.8.1 Reporting

6.8.1.1

A distributor shall report to the Board on the status of cyber security readiness referencing the Cyber Security Framework at such times and in such a manner as may be directed by the Board.

6.8.1.2

The Chief Executive Officer of the distributor shall certify the distributor's reported cyber security readiness in such a form as may be required by the Board.

6.8.2 Continuing Obligations Re-Distribution System and Privacy

Nothing in this section shall limit any obligations of a distributor to maintain the reliability and integrity of its distribution system, and to protect personal information.

Attachment C -

Notice of Amendments to the Transmission System Code and the Distribution System Code and Notice of Proposal to Amend the Transmission System Code and the Distribution System Code

March 15, 2018

EB-2016-0032

Comparison Version of Amendments

Note: Additions (underlined) and deletions (stricken through) indicated changes to the amendments relative to the amendments as they were proposed on December 20, 2017. The text of the Amendments is set out in italics below, for ease of identification only.

A. Amendments – Definitions (TSC section 3B.2.1)

"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access. Cyber security includes ~~both~~ electronic and physical security issues as they related to cyber security protection.

B. Amendments – Definitions (DSC section 1.2)

"Cyber Security" means a body of technologies, processes, and practices designed to protect networks, computers, programs, data and personal information from attack, damage or unauthorized access. Cyber-security includes ~~both~~ electronic and physical security issues as they related to cyber security protection.