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

December 20, 2017

NOTICE OF PROPOSAL TO AMEND A CODE

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

BOARD 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) is giving notice under section 70.2 of the *Ontario Energy Board Act, 1998* (Act) of proposed amendments to the Transmission System Code (TSC) and the Distribution System Code (DSC).

A. Purpose

The purpose of the proposed TSC and DSC amendments is to establish regulatory requirements for all licensed transmitters and distributors to provide the OEB with information to demonstrate that they are taking appropriate actions relative to their cyber security risks. In the absence of a recognized electricity transmission/distribution standard or framework, the amendments rely on the establishment and use of the industry-developed[1] Ontario Cyber Security Framework (Framework)[2], as the common

[1] Industry development of the Framework was through the Cyber Security Working Group (CSWG).
[2] Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets (the Framework).

basis for assessing and reporting cyber security capability to the OEB.

By reporting cyber security readiness against consistent criteria, the OEB will have greater confidence that the reported state of cyber security in the electricity sector is comparable and understood.

B. Summary

With respect to cyber security, the OEB expects every licensed transmitter and distributor to manage its business in a manner that achieves the reliability, security and privacy protection obligations that are set out in its licence and related regulatory requirements. Each licensed entity is responsible to meet its obligations and to have the technical expertise in relation to cyber security. The assessment of distributors and transmitters actions in terms of meeting these obligations has become more important with the increase in data gathering to support customer choice and innovation in technology to operate the networks in more efficient manners, and in the modernizing of the electricity grid.

The OEB expressed the view in its *Supplemental Report on Smart Grid* that*"…The Board will not develop its own set of cyber-security and privacy standards but instead, will require regulated entities to provide evidence of meeting appropriate cyber-security and privacy standards…"*[3]. Consistent with this view, the OEB will rely on an industry developed framework that continuously evolves to meet cyber security needs. This approach is consistent with the OEB's expectations that licensed transmitters and distributors adopt good utility practice that reflects the best practices in their sectors.

In order to achieve this outcome the OEB engaged in a consultation with distributors, transmitters and industry cyber experts that developed an industry designed Framework to assess cyber security maturity and readiness. The Framework strikes a balance by providing a methodology that is both descriptive and guiding. In doing so, combined with the knowledge gained through information sharing, licensed transmitters and distributors have the freedom to assess their risk appetite in an informed manner, and to interpret and apply operational controls that satisfy objectives reflected in the Framework, external developments and their own business decisions.

The awareness of risks and sharing of intelligence about cyber issues is essential to understanding effectively using the Framework as an assessment tool. Reporting of cyber security maturity will incorporate an expectation that licensed transmitters and

---

[3] EB-2011-0004 – *Report of the Board – Supplemental Report on Smart Grid*, p.19 issued February 2013

distributors will confirm active information sharing. Through the exchange of knowledge and experience and the assessment against the framework licensed transmitters and distributors will be able to demonstrate good utility practice in their reporting to the OEB.

At the same time, the OEB is of the view that sector readiness needs to be underpinned by Code obligations being placed on licensed transmitters and distributors with regard to matters such as the use of the Framework in supporting their reporting.

The OEB believes this proposed approach strikes an appropriate balance and is consistent with stakeholder input that has been received to date. Attachments A and B to this Notice contain the proposed amendments to the TSC and DSC, respectively.

C. Background

On February 11, 2016, the OEB initiated a policy consultation[4] to review the state of cyber security of the (non-bulk) electrical grid[5] and natural gas distribution system and associated business systems.

Ontario transmitters are required to comply with the existing cyber security standards for the bulk transmission system that were established by the North American Electric Reliability Corporation as part of its Critical Infrastructure Protection initiative.

Early research undertaken by OEB staff confirmed that a non-bulk electricity transmission system and distribution-focused framework or standard for cyber security did not exist. Ontario licensed distributors and transmitters have undertaken the selection and interpretation of generic cyber security standards in an attempt to develop a cyber-security capability that is appropriate for their perceived level of risk. As a result, the OEB is not able to assess if utilities have been taking reasonable actions on a consistent and measurable basis. The OEB understands there may already be an appropriate standard regarding cyber security for natural gas distributors (see section F of this Notice) and is therefore only addressing non-bulk electricity systems operated by licensed transmitters and distributors in these proposed code amendments.

Designing a Cyber Security Framework

Given the lack of an accepted standard, the OEB determined that it would undertake

---

[4] In this letter, the OEB indicated it would work with key industry stakeholders via the CSWG to establish a common framework referencing recognized industry standards, policy guidelines and auditing requirements and to further define the requirements for meeting their licensing obligations for system reliability and consumer privacy in a cost efficient manner.

[5] Cyber security standards have already been established at the bulk transmission system level by the North American Electric Reliability Corporation (NERC) that regulated transmitters must comply with.

discussions with licensed transmitters and distributors, as well as other stakeholders, to develop an industry based framework for the assessment of actions licensed entities are taking to address cyber security.

The OEB established a Cyber Security Working Group (CSWG) made up of distributors, transmitters and other key stakeholders, as well as an expert consulting team to support the work. The CSWG's mandate was to develop the initial framework and set the foundation for the long-term, sustainable objective of having the sector assume overall accountability for the management and evolution of the framework. The CSWG held extensive meetings and undertook research regarding the practices of Ontario licensees based on which the CSWG developed the proposed *Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets*.

An OEB Staff Report[6] was prepared that set out staff's view on cyber security, OEB expectations and views on the proposed Framework including the benefits of the approach developed by the CSWG. On June 1, 2017, the Staff Report, the industry-developed proposed Framework and a related White Paper[7] were issued for broader stakeholder comment.

On July 15, 2017, the OEB received 15 submissions in response to those documents. Stakeholders were generally supportive of the establishment of a common Framework and saw this as a positive policy initiative, particularly that it was developed by industry, through a highly interactive and collaborative approach. Stakeholders' views on specific issues are addressed in the relevant section of this Notice.

The feedback from stakeholders has been considered and incorporated into this Notice. As well the CSWG was asked to review to the stakeholder comments on the proposed Framework and consider the issues that had been raised. After meeting to discuss the feedback the CSWG prepared a revised Framework and implementation recommendations. The revised Framework and implementation guidance are set out in Appendix C to this Notice. The CSWG also prepared a summary of its recommendations in response to the comments, the Assessment Report, which has also been posted on the OEB's website to provide an explanation of changes made to the Framework in response to comments.

---

[6] *Staff Report to the Board on a Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors* (Staff Report) and *White Paper* (draft Framework).
[7] *Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets*.

The Cyber Security Framework

The Framework has been developed by the CSWG as a guide to assessing the cyber security and privacy maturity of Ontario's electricity transmitters (with respect to non-bulk assets) and distributors. The Framework, supporting tools and mechanisms are objectives-based and provide transmitters and distributors with operational flexibility to implement cyber security measures that they deem necessary to meet their cyber security and privacy obligations. The structure of the Framework leverages well accepted critical infrastructure and privacy protection approaches and includes sector-specific context. It provides a methodology and tools to assess inherent risk, define the licensee's benchmark objectives and measure progress toward those objectives.

The Framework relies on a set of questions which guide a transmitter or distributor in assessing and determining their inherent risk level. The risk level is aligned with a recommended set of cyber security objectives that would be appropriate for that level of risk. The Self-Assessment Questionnaire (SAQ) provides a consistent approach for self-assessments to compare their actual cyber maturity level to the recommended objectives, and thus identify gaps. The results can be used to inform the transmitters' or distributors' plans to address cyber security and privacy threats (including those that result from interactions with their service providers[8] and interconnected customers[9]) and forms the basis of reporting their cyber protection readiness. This approach will ensure consistency in assessing maturity, identifying gaps and support peer collaboration.

The benefits of the Framework identified by the CSWG are:

- It leverages authoritative approaches (NIST and ES-C2M2) that are being used by an increasing number of critical infrastructure operators.
- It integrates privacy principles (PbD)[10].
- It incorporates sector-specific attributes that focus the application of NIST[11] to the distribution sector through a set of tools and mechanisms.
- It is scalable so that cyber maturity aligns with risk.
- It proposes a set of benchmark control objectives for different risk levels.

---

[8] Service Providers refers to third parties entities that provide services to the distributor supporting their ongoing operations.
[9] Interconnected Customers refers to companies that interact with the distribution system, such as generators and load customers.
[10] PbD – Privacy by Design
[11] NIST - National Institute of Standards and Technology.

- It provides distributors with flexibility in how they achieve their cyber security objectives.
- It can be used to support transmitter and distributor governance.

Broad support was expressed by the electricity sector for the adoption of the NIST framework as it is seen to be flexible, and descriptive in nature, allowing for different implementation strategies. Several stakeholders also noted that the Framework provided enhanced and consistent protection of data privacy; using PbD and C2M2[12] as "core elements" to augment the management of risk.

The OEB appreciates the valuable work of the members of the CSWG on behalf of the industry. The extensive discussions, research and analysis has provided a robust initial Framework that reflects industry best practices as well as learnings from the work Ontario utilities have already undertaken. The OEB is of the view that the Framework as revised by the CSWG provides a basis for the assessment of licensed transmitters and distributors actions to ensure that the systems they operate are adequately protected and achieving the OEB's expectations with respect to cyber security and protection of privacy. The proposed Code amendments require that licensed transmitters and distributors use the current version of the Framework as the basis for reporting on the state of their cyber security readiness and capability.

Information Sharing

Increased sophistication and frequency of cyber-attacks has heightened the need to have an effective and dynamic cyber security strategy. Transmitters and distributors will be challenged to keep abreast of the risks and develop strategies to maintain their cyber security capability individually. Supported by stakeholder feedback, the OEB is of the view that a cyber-security information sharing approach that leverages the experience of the sector will enhance their efficiency and efficacy in responding to cyber security threats.

While security collaboration is already occurring in Ontario, it is doing so on an *ad hoc* basis as issues arise, including through voluntary mechanisms such as the cyber security forum led by the IESO. As the CSWG has identified the core benefits of a structured information sharing mechanism should include:

- Developing community oversight and governance structures aligned to distributor needs;

---

[12] Electricity Subsector Risk Management Process and the Cybersecurity Capability Maturity Model -ES-C2M2

- Creating a central and secure ability to share information;
- Establishing cross-sector sharing as a priority to foster industry-specific intelligence with appropriate controls and agreements in place; and
- Enable industry to gather and analyze intelligence shared across Ontario's energy sector while ensuring promoting greater awareness of licencees through sharing best practices, concerns and discussion items relevant to Ontario's energy sector.

In supporting open discussions on threat intelligence and strengthening the collective cyber threat intelligence capability among licensed transmitters and distributors, the OEB is of the view that the sharing of information should be based on best practices. Protocols such as The Canadian Cyber Threat Exchange (CCTX) reporting best practices and the use of Traffic Light Protocol (TLP)[13] are two such approaches that could be considered, in establishing its information sharing approach.

The OEB is of the view that involvement in such an information sharing approach is necessary for any regulated entity to be aware of the evolving landscape and is essential to being able to assess their cyber security risks and take appropriate actions to address any gaps, and certify their cyber security maturity. Further, participation in information sharing is a sign of good utility practice that has, as the OEB has learned, been adopted by many of the licensees to date.

In order to achieve the benefits that have been identified from robust information sharing among sector entities, the OEB is of the view there needs to be a central agency that provides this service to all licensed transmitters and distributors. This approach would also lead to greater efficiency in implementation. The OEB expects licensed transmitters, distributors and the IESO to develop an effective manner to institutionalize information sharing so that it achieves the benefits.

Implementation Considerations

Stakeholder feedback has suggested that implementation assistance, support and guidance would enhance the efficacy of incorporating the Framework into the

[13] The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. It is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared. Each level carries increased risk to privacy or operations if misused: 'White'- data that can be shared share with anyone, 'Green' (shared only with peers, and not via publicly accessible channels0- 'Amber'- (shared only with those known in its trusted community, and who need to know); and 'Red' (limited distribution, unless it is urgent).

transmitters and distributors' cyber security strategies and reporting. During implementation discussions, the CSWG has also indicated that it is critical that a coordinated approach to the rollout of the Framework is necessary to maintain the momentum that is already in the sector. In the Assessment Report, the CSWG has outlined their recommendations on how to proceed with an effective implementation including key actions for success that include:

- Focussed support in conducting early adopter implementation in order to identify and provide common guidance to the other licensees.
- Leveraging industry forums, user groups and associations, by establishing a coordinated approach to support transmitters and distributors as needed.
- Provision of educational materials to enhance understanding and implantation guidebooks.
- Peer mentoring.

Some stakeholders have recommended that the OEB place a temporary moratorium on finalizing the details related to the implementation and compliance to allow the industry to advance at a 'measured pace' and allow for early experience to incorporate lessons learned and insights. Stakeholders have expressed concerns that the Framework has not been fully tested in order to calibrate the assessment approach. The CSWG has responded by revising the Framework, incorporating stakeholder comments and performing further tabletop testing. The OEB acknowledges that while the CSWG developed Framework, incorporates the best practices of the industry it 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 the implementation of reporting requirements. Further the OEB remains of the view that ongoing implementation is best developed and led by industry. The OEB acknowledges the concerns about implementing the Framework and reporting, and therefore intends for the CSWG to remain in place, to support implementation efforts, until the industry forums and associations are able to take the lead. The OEB will facilitate meetings if needed, to support the sector in establishing a coordinated approach to the implementation of the Framework.

Framework Evolution

Stakeholders in their comments expressed concerns about the nature and cost implications of recommendations related to the future development phases, contained in the proposed Framework. Stakeholders sought clarifications related to the development of the risk indicators, tracking, retention and publication of reporting. Similarly, clarity around how compliance would be addressed; the role of the OEB would play in the collection of detailed information; and independent audit requirements was sought.

The CSWG has reflected on the stakeholder feedback, but continues to believe that their recommendations have merit, and can form the basis of the further evolution of the Framework. Five recommendations were provided by the CSWG to industry to consider, as it evolves the Framework:

- Increasing the maturity level requirements over time, for all risk profiles,
- Incorporating Key Risk Indicator metrics.
- Establishing a central compliance authority to compile additional details related to each licenced transmitter and distributor.
- Establishing requirements for independent audits.
- Enhancing reporting to the OEB, related to efforts by licensees to reduce their residual risks.

The OEB acknowledges the effort that the CSWG has put into providing future-looking aspirational goals and recognizes that, as the sector evolves, these concepts could be examined as part of further industry work to advance the Framework. It is recognized that much more work will be required by industry in these areas before proposing the incorporation of some of the changes into the Framework. The OEB confirms its view that licensees are responsible to manage their businesses in a manner that achieves the licencee's reliability, security and privacy obligations. Many of the recommendations reflect broader sector risks that are associated with the nature of interconnectivity between transmitters and distributors. The OEB expects the industry to work, through an appropriate forum to evolve the Framework in a collaborative manner and incorporate any of these recommendations when, and if it is felt that it will enhance achieving licensees' ability to meet their obligations.

D. Proposed TSC Amendments

Definitions (new section 3B.2.1)

In order to support the proposed TSC and DSC amendments set out in this Notice, the OEB is proposing to add a number of definitions to both Codes. These definitions capture the key concepts related to the implementation of the cyber security policy, specifically:

- A description of Cyber Security.
- A definition of the Framework.

Reporting (new section 3B.2.2)

The OEB will require that licensed transmitters report their cyber security maturity based on their assessment against the Framework, and provide the necessary information and certification to the OEB on an annual basis. The Code amendments require the form of

assurance be provided through a self-certification report signed by the Chief Executive Officer (CEO) of the licensee.

Details of the reporting requirements will be established in the OEB's *Reporting and Record Keeping Requirements* (RRR). The OEB intends to work with licensed transmitters and distributors to develop the certification requirements. It is envisioned that this will be comprised of two parts.

- The first will focus on confirmation that the Framework's process and assessments have been carried out. The report will include the results such as the risk level, statement of the current maturity relative to the baseline objectives, and an indication of the plans to address gaps that have been identified; and
- The second part will include responses to a series of questions that the OEB will develop in order to understand the transmitter's cyber security approach. Subjects may cover areas such as risk management and governance approaches; planning and incident response and recovery; information sharing partnerships; procurement practices; education; and testing.

The OEB will use the report to assess the transmitter's cyber security readiness and identify possible concerns for follow up, including through the OEB's annual audit program.

The OEB is proposing that an initial report is submitted to the OEB three (3) months after these Code amendments come into force. The OEB believes this initial report will ensure all licensed transmitters have reviewed and understood the Framework, and are taking steps to assess their cyber security readiness against the Framework. The intended form of the initial report accompanies this Notice as Attachment D.

Following the initial report, the OEB is proposing that the transmitter self-certify on an annual basis, in a manner that aligns with the OEB's RRR. Annual self-certification of cyber security capability would be required starting in 2019, with details to be worked out through the development of the reporting and certification processes.

The OEB is of the view that ongoing annual certification reporting is necessary to provide the OEB with an understanding of cyber security maturity and readiness and continual improvement, compared to the Framework. As a consequence, the OEB is proposing to add section 3B.2.2 to the TSC to include self-certification reporting requirements for transmitters, on an initial and ongoing annual basis as discussed above.

The OEB requires regulated entities to maintain records and provide such information as the OEB may require from time to time. Supporting documentation in relation to the

self-certification is expected to be archived, consistent with the record retention policy[14] for regulated entities.

The OEB acknowledges that cyber security reports which it receives from transmitters and distributors will contain sensitive information. The OEB will treat the reports filed in confidence and segregate them from other Board records. Access to the reports will be limited to individuals who require access as part of their employment with the OEB.

Continuing Obligations re Transmission System and Privacy (3B.2.3)

The establishment of the OEB reporting requirements, the Framework, and participation in information sharing are tools to enhance the overall understanding of cyber security within the electricity sector. The transmitter is obligated through its licence and related regulatory requirements to maintain the reliability and integrity of its transmission system. The adherence to minimum cyber security expectations as set out in the Code amendments does not absolve the transmitter from assessing the risks and taking further action to manage its overall risk portfolio.

The OEB is, therefore, proposing to add section 3B2.3 to the TSC.

Proposed DSC Amendments

Definitions (section 1.2)

Subject to such modifications required to reflect distributors and the distribution system, as opposed to transmitters and the transmission system, the OEB is proposing to add the same definitions to the DSC as those proposed for the TSC as set out above,

Reporting (new section 6.8.1)

Subject to such modifications as may be required by the context, the OEB is proposing to add the same language to the DSC as is it is proposing for the TSC.

Continuing Obligations re Distribution System and Privacy (new section 6.8.2)

Subject to such modifications as may be required by the context, the OEB is proposing to add the same language to the DSC as is it is proposing for the TSC.

---

[14] EB-2015-0247 - Mandatory Record Retention Period for Regulated Entities

E. Benefits and Costs

The OEB believes the Code amendments set out in this Notice will result in benefits that exceed any additional costs. Overall the Code amendments will result in the OEB being more informed about the cyber readiness of the sector and its ability to protect the privacy of consumers' information. This will lead to greater consumer acceptance of the innovations in data gathering and new services that make use of their electricity usage information.

The OEB believes these Code amendments will achieve the following beneficial outcomes:

- Transmitters and distributors can cost-efficiently increase their cyber security capabilities through collaboration and sharing of experiences and best practices.
- Reporting against a reference Framework will provide a comparative assessment of transmitter and distributor cyber security capabilities.
- Trust and transparency within the energy sector will be strengthened, and regulated entities will be able to provide measurable representations to the OEB that regulated entities are taking what they consider to be appropriate action with respect to their security, reliability and privacy obligations.
- The ongoing evolution of the Framework will provide a valuable guide to support transmitter and distributor cyber security maturation.

The OEB expects that information sharing among transmitters and distributors will result in a stronger sector capability, through collaboration and sharing of experiences and solutions. With the sector pooling their skills and experience, there will be a reduced need for individual developments by leveraging commonly developed solutions. Recognizing the close inter-relationships that occur between connected transmitters and distributors, this approach is expected to support and improve all participants and start to address the weakest links in the integrated grid. Achievement of such an outcome will enhance cyber security capabilities at a lower cost to consumers while providing solutions through economies of scale. The OEB intends to work with the sector and the IESO to develop appropriate mechanisms to support this important activity.

The establishment of the Framework leverages industry best practices and leading international references, and provides a consistent toolset and process as a guide to enhance cyber security within the sector. The Framework provides transmitters and distributors that do not have extensive cyber security expertise with a roadmap to address cyber security. The tools and mechanisms included in the Framework enable cross-references to exist general cyber security standards and frameworks that are

being interpreted by individual transmitters and distributors, and as such may not require changes to the approaches they are currently undertaking. Being objectives based, it provides operational flexibility to implement cyber security measures that transmitters and distributors deem necessary to meet their reliability, security and privacy obligations.

Some stakeholders raised concerns that the Code amendments and in particular the requirement to use the Framework as a basis for assessing their cyber security readiness would impose 'more stringent requirements', and thus costs upon larger LDCs than all LDCs on average. The OEB believes that transmitters and distributors should have already incorporated cyber security into their business and asset planning, consistent with their risk portfolio. Where cyber security has been implemented, the Framework and the OEB's requirement to certify against it, is expected to provide another perspective on the level of cyber security maturity. An assessment of current cyber security against the Framework is anticipated to identify areas where further cyber security actions would enhance and align risk and maturity. Increased awareness of this risk aspect, may change the prioritization of investments, and result in redirection of funds.

It is the OEB's expectation that transmitters and distributors will incorporate additional cyber security investments into their transmission or distribution system plans, the filing of which is already required by the OEB, and that related expenditures will be addressed in the course of their revenue requirement and rate applications to the OEB.

F. Natural Gas Distributors

Through the consultations, the OEB has learned that unlike the situation in electricity, there does appear to be an accepted standard for addressing cyber security in the natural gas sector, the Security Management for Petroleum Natural Gas System standard (Z246.1)[15]. The OEB understands that the Technical Standards and Safety Authority (TSSA) has a role in overseeing cyber security for natural gas distributors. Further discussions with the TSSA and natural gas distributors are planned in order to assess opportunities to share compliance information to avoid any regulatory overlap. Once those discussions are complete the OEB will assess the need for any regulatory requirements for the natural gas distributors.

[15] Security Management for Petroleum Natural Gas System standard Z246.1

G. Coming into Force

The OEB proposes that the proposed amendments to the TSC and DSC, as set out in Attachments A and B will come into force on the day that the final Code amendments are published on the OEB's website after having been made by the OEB.

Interim reporting by regulated electricity transmitters and distributors related to cyber security self-assessment would be required within three (3) months after the Code amendments are in force. Annual self-certification of cyber security capability would be required starting in 2019.

H. Cost Awards

Cost awards will be available under section 30 of the *Ontario Energy Board Act, 1998* to eligible persons in relation to the provision of comments on the proposed amendments, **to a maximum of 15 hours**. Costs awarded will be recovered from all rate-regulated licensed electricity distributors and transmitters based on their respective distribution revenues.

Appendix A to this Notice contains important information regarding cost awards related to these proposed Code amendments, including in relation to eligibility requests and objections. In order to facilitate a timely decision on cost eligibility, the deadlines for filing cost eligibility requests and objections will be strictly enforced.Invitation to Comment

All interested parties are invited to submit written comments on the proposed amendments to the TSC and DSC as set out in Attachments A and B by **January 18, 2018**.

Filings should be sent to:

Kirsten Walli
Board Secretary
Ontario Energy Board
P.O. Box 2319
2300 Yonge Street, Suite 2700
Toronto, Ontario, M4P 1E4

The OEB requests that interested parties make every effort to provide electronic copies of their filings in searchable/unrestricted Adobe Acrobat (PDF) format, and to submit their filings through the OEB's web portal at https://www.pes.oeb.ca/eservice. A user ID is required to submit documents through the OEB's web portal. If you do not have a user ID, please visit the "e-filings services" webpage on the OEB's website at

www.oeb.ca, and fill out a user ID password request.

Additionally, interested parties are requested to follow the document naming conventions and document submission standards outlined in the document entitled "RESS Document Preparation – A Quick Guide" also found on the e-filing services webpage. If the OEB's web portal is not available, electronic copies of filings may be filed by e-mail at boardsec@oeb.ca.

Filings to the OEB must be received by the Board Secretary by **4:45 p.m.** on the required date. They must quote file number EB-2016-0032 and include your name, address, telephone number and, where available, your e-mail address and fax number.

If the written comment is from a private individual (i.e., not a lawyer representing a client, not a consultant representing a client or organization, not an individual in an organization that represents the interests of consumers or other groups, and not an individual from a regulated entity), before making the written comment available for viewing at the OEB's offices or placing the written comment on the OEB's website, the OEB will remove any personal (i.e., not business) contact information from the written comment (i.e., the address, fax number, phone number, and e-mail address of the individual).

However, the name of the individual and the content of the written comment will be available for viewing at the OEB's offices and will be placed on the OEB's website.

This Notice, including the proposed amendments to the TSC and DSC, set out in Attachments A and B, supporting information including the Framework and all written comments received by the OEB in response to this Notice will be available for public viewing on the OEB's website at www.oeb.ca and at the office of the OEB during normal business hours.

Any questions regarding the proposed amendments to the Codes described in this Notice should be directed to IndustryRelations@oeb.ca , or by phone at 416-314-2455 or 1-888-632-6273 (the OEB's toll-free number).

DATED at Toronto, December 20, 2017

ONTARIO ENERGY BOARD

Original signed by

Kirsten Walli
Board Secretary

Appendix A

Notice of Proposed Amendments to the Transmission System Code and the Distribution System Code

December 20, 2017

EB-2016-0032

Cost Awards

Cost Award Eligibility

Any person intending to request an award of costs must file with the OEB a written submission to that effect by **January 4, 2018**, identifying the nature of the person's interest in this process and the grounds on which the person believes that it is eligible for an award of costs (addressing the cost eligibility criteria as set out in section 3 of the *Practice Direction on Cost Awards*). An explanation of any other funding to which the person has access must also be provided, as should the name and credentials of any lawyer, analyst or consultant that the person intends to retain if known. All requests for cost eligibility will be posted on the OEB's website.

Rate-regulated licensed electricity transmitters and distributors will be provided with an opportunity to object to any of the requests for cost award eligibility. If an electricity transmitter and distributor has any objections to any of the requests for cost eligibility, those objections must be filed with the OEB by **January 10, 2018**. Any objections will be posted on the OEB's website. The OEB will then make a final determination on the cost eligibility of the requesting participants.

Cost Eligible Activities and Hours

Cost awards will be available in relation to the provision of comments on the proposed amendments to the TSC and DSC to a **maximum of fifteen (15) hours**.

Cost Awards

When determining the amount of the cost awards, the OEB will apply the principles set out in section 5 and 6 of its *Practice Direction on Cost Awards*.. The maximum hourly rates set out in the OEB's Cost Awards Tariff will also be applied. The OEB expects that

groups representing the same interests or class of persons will make every effort to communicate and coordinate their participation in this process. Interested parties are reminded that cost awards are made available on a per eligible participant basis, regardless of the number of professional advisors that an eligible participant may wish to retain.

The OEB will use the process set out in Section 12 of its *Practice Direction on Cost Awards* to implement the payment of the cost awards. Therefore, the OEB will act as a clearinghouse for all payments of cost awards in this process.

Attachment A -

Notice of Proposed Amendments to the Transmission System Code and the Distribution System Code

December 20, 2017

EB-2016-0032

Proposed Amendments to the Transmission System Code

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

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 both electronic and physical security.

"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 Proposed Amendments to the Transmission System Code and the Distribution System Code

December 20, 2017

EB-2016-0032

Proposed 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 both electronic and physical security

"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 Proposed Amendments to the Transmission System Code and the Distribution System Code

December 20, 2017

EB-2016-0032

Ontario Cyber Security Framework

- Framework
- Risk Profile Tool
- Self-Assessment Questionnaire (SAQ)

Attachment D –

Notice of Proposed Amendments to the Transmission System Code and the Distribution System Code

December 20, 2017

EB-2016-0032

Certification of Compliance Report

Cyber Security Framework Certification of Compliance Report

(*Confidential)*

Date:

Based on the results dated *(completion date)*, the signatories identified below assert the following interim report for the entity as of *(date)*: (***check one):***

Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☐ I have read, reviewed and understood the Cyber Security Framework.

☐ I have assigned a team to assess the current cyber security capability against the Framework, in order to identify any gaps

☐ I have prepared a plan to be able to certify my cyber security capability against the Framework.

☐ I have taken steps to incorporate information sharing actions in order to increase knowledge of threats and solutions, and share lessons learned.

Interim Report Acknowledgement

Signature of Licensee Chief Executive Officer *Date:*

Licensee Chief Executive Officer Name: *Title:*