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

BY EMAIL AND WEB POSTING

February 12, 2024

NOTICE OF PROPOSAL TO AMEND A CODE

PROPOSED AMENDMENTS TO THE TRANSMISSION SYSTEM CODE AND THE DISTRIBUTION SYSTEM CODE TO ENHANCE CYBER SECURITY READINESS
BOARD FILE NO.: EB- 2023-0173

To: All Licensed Electricity Distributors
All Licensed Electricity Transmitters
Independent Electricity System Operator

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) to enhance cyber security readiness in Ontario's electricity sector. The proposed amendments will come into force on **October 1, 2024**.

The proposed amendments require licensed electricity transmitters and distributors (utilities) to comply with a new Ontario Cyber Security Standard (Standard) document. The Standard sets out specific cyber security readiness requirements. Transmitters and distributors are expected to manage their business risks including the risks due to cyber threats. The OEB is proposing these amendments to enhance cyber security in the electricity sector given the potential for heightened cyber security risk as the energy transition proceeds and as new technologies are integrated into Ontario's electricity system.

The initial cyber security requirements focus on privacy, corporate governance and situational awareness related to cyber security. The OEB considers these to be foundational elements to enhancing and strengthening utility cyber security readiness. The privacy and governance requirements reinforce the protection of personal information and organizational decision making, respectively. The situational awareness requirement will provide utilities with access to cyber security intelligence, tools and related products. Setting these compliance requirements for utilities aligns with the OEB's strategic goal of protecting the public. Building on existing reporting requirements, the OEB expects these requirements will improve utilities' resilience in the face of an ever-evolving cyber security threat landscape.

A. Background and Rationale

On March 15, 2018, the OEB amended the TSC and the DSC to include cyber security reporting expectations. Every April, since 2019, utilities have been required to report to the OEB on the status of cyber security readiness as part of the OEB's *Reporting and Record-keeping Requirements* (RRR) submissions.

On February 7, 2023, the OEB issued a letter describing a plan to implement cyber security requirements that support utilities in enhancing their cyber security readiness. The letter noted that licensed utilities are responsible for managing cyber security risk as part of their overall business risk and that the OEB's role is to set the expectations for managing those risks.

The Cyber Security Advisory Committee (CSAC) is an industry-led committee consisting of representatives of Ontario's electricity utilities who are directly engaged in their companies' cyber security activities. The CSAC's role is to provide the OEB with expert advice and to maintain and evolve the Ontario Cyber Security Framework (OCSF). Over the course of 2023, OEB staff engaged with the CSAC about the requirements described in the February letter.

On December 19, 2023, the OEB notified licensed utilities that the CSAC had released version 1.1 of the OCSF. The OEB considers the OCSF to be the critical tool for utilities to assess their cyber security readiness. The OCSF consists of more than 100 control actions that are classified into five functions: Identify, protect, detect, respond, and recover. The OCSF is based on the National Institute of Standards and Technology (NIST) cyber security framework, which is a widely referenced cyber security framework. It also incorporates privacy principles contained in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). The RRR and the cyber security sections of the TSC and DSC, respectively, reference the OCSF as being the basis for utility cyber security reporting to the OEB.

Approach to Amendments

In proposing these amendments, the OEB is guided by its objectives as set out in section 1 of the Act. The OEB believes that the proposed amendments will better protect the public interest by enhancing utility resilience and reinforcing the OEB's monitoring of utility compliance with existing customer information security expectations. These amendments will also facilitate cyber security related collaboration and innovation in the electricity sector.

The Standard

The proposed TSC and DSC amendments require licensed utilities to comply with the Standard, which sets out specific cyber security readiness requirements.

A code issued under section 70.1 of the Act may incorporate by reference, in whole or in part, any standard, procedure or guideline.[1] The Standard does not form part of the DSC or TSC and is not subject to the requirements of section 70.2 of the Act. Although the Standard is not part of the TSC or DSC, the Standard is provided for information in Appendix E to this Notice.

With a separate Standard, the OEB will be able to modify cyber security requirements more nimbly in response to developments in industry standards and changing cyber security risks. The core regulatory requirement for compliance with the Standard will remain as set out in the TSC and DSC. The Standard will be more accessible as a stand-alone document and will provide a common set of requirements. The OEB expects that the adaptability and accessibility of the Standard will allow it to develop into a key cyber security reference document for utilities. The OEB expects to engage with utilities, primarily through the CSAC, on future amendments to the Standard.

Initially, the Standard will:

a) make participation in the Independent Electricity System Operator's (IESO) Lighthouse information sharing and situational awareness service mandatory for all licensed transmitters and distributors; and
b) make specific governance and privacy related portions of the OCSF mandatory for applicable transmitters and distributors.

Transmitters and distributors currently report on their Lighthouse participation status and their implementation of the OCSF, including the governance and privacy related portions, as part of the RRR. Therefore, the new requirements are an incremental change to require compliance with specific elements.

Lighthouse Service Participation

On July 19, 2018, the OEB amended the licence of the IESO to require the IESO to provide information sharing and situational awareness services to Ontario utilities. In response, the IESO developed and operates the Lighthouse service, which is made available to Ontario utilities at no cost.

Utility CEOs and senior executives have advised OEB staff that the Lighthouse service is useful. Having uniform participation across the sector will enhance cyber security

[1] See subsection 70.1(4) of the Act.

readiness by ensuring that all utilities have access to the Lighthouse service information.

Participation in the Lighthouse service involves three steps:

i) signing the participation agreement provided by the IESO;

ii) being granted access to the Lighthouse Member Portal by the IESO; and

iii) establishing a secure network connection with the IESO's Lighthouse solution infrastructure.

Governance and Privacy Related Portions of the OCSF

The cyber security industry has identified cyber security governance as being the foundation of cyber security excellence. Ontario utility CEOs and senior executives advised OEB staff that they share this view. The growth in cyber security threats has also increased the risk to the privacy and security of consumer information, which licensed utilities are required to maintain. For these reasons, the OEB is proposing to make certain cyber security governance and privacy related control actions mandatory.

The specific control objectives being included in the Standard have been part of the OCSF since 2018. They call for utilities to develop cyber security policies, roles and responsibilities, and processes to aid the identification, assessment, and management of cyber security risks.

B. Proposed Amendments to the TSC

Appendix A to this Notice contains the proposed amendments to the TSC, and Appendix B contains a clean version of the relevant provisions of the TSC as they would appear if all proposed amendments were adopted.

C. Proposed Amendments to the DSC

Appendix C to this Notice contains the proposed amendments to the DSC, while Appendix D contains a clean version of the relevant provisions of the DSC as they would appear if all proposed amendments were adopted.

D. Anticipated Costs and Benefits

The OEB expects the costs of implementing the Standard to be minimal. It is the OEB's understanding that most licensed utilities already participate in the Lighthouse service and it is provided at no cost.

Lighthouse portal access does not require capital investment. It is the OEB's understanding that establishing a secure network connection with the IESO's

Lighthouse solution infrastructure may, in some cases, require capital investment, but the OEB does not expect this investment to be material. The OEB does not expect these steps to cause significant incremental administrative expenses.

As noted above, the Framework's privacy and cyber security governance control actions typically consist of policies, processes and structures. The OEB expects utilities to be able to develop and implement these requirements without causing significant incremental administrative expenses especially considering they have been reporting against these OCSF control objectives for several years. Capital investments are not required to implement these control actions.

The OEB therefore expects that any incremental costs transmitters and distributors may incur will be exceeded by the benefit of enhanced cyber security readiness that will come from participation in the Lighthouse service and the implementation of governance and privacy control objectives.

E. Coming into Force

The OEB proposes to have the amendments come into force on **October 1, 2024** in recognition of the time needed by some utilities to comply with them. Ongoing compliance with the proposed amendments and the Standard will be assessed through the cyber security reports submitted to the OEB by each transmitter and distributor every April as part of the RRR. Questions 1.a), 1.b), 2.a) and 4.a) of the Cyber Security Readiness Report in April 2024 will be aligned with the requirements in section 3 and section 4 of the proposed Standard. For clarity, the cyber security reports to be submitted by each transmitter and distributor in April 2024 need not demonstrate compliance with the proposed amendments and the Standard because the April 2024 submissions are reporting on the 2023 reporting period. However, the OEB anticipates that many transmitters and distributors were already compliant in 2023 with the proposed amendments and the Standard and that this will be demonstrated in their April 2024 submissions.

Those transmitters and distributors that submit a cyber security report in April 2024 which does not include a 'Yes' response to questions 1. a), 1. b), 2. a) and 4. a) will be required to submit an interim report in October 2024. This interim report will involve those transmitters and distributors providing updated responses to questions 1. a), 1. b), 2. a) and 4. a) as of the effective date of the proposed amendments. Instructions for submitting the interim report will be provided closer to October.

F. Invitation to Comment

The OEB invites comments from any interested stakeholder on the proposed amendments and the Standard. Anyone interested in providing written comments is

invited to submit them by **March 5, 2024**. Your written comments must be received by the Registrar by **4:45 p.m.** on that date.

Instructions for Submitting Comments

Stakeholders are responsible for ensuring that any documents they file with the OEB **do not include personal information** (as that phrase is defined in the *Freedom of Information and Protection of Privacy Act*), unless filed in accordance with rule 9A of the OEB's Rules of Practice and Procedure.

Please quote file number, **EB-2023-0173** for all materials filed and submit them in searchable/unrestricted PDF format with a digital signature through the OEB's online filing portal.

- Filings should clearly state the sender's name, postal address, telephone number and e-mail address
- Please use the document naming conventions and document submission standards outlined in the Regulatory Electronic Submission System (RESS) Document Guidelines found at the Filing Systems page on the OEB's website
- Stakeholders are encouraged to use RESS. Those who have not yet set up an account, or require assistance using the online filing portal can contact registrar@oeb.ca for assistance

This Notice, including the proposed TSC amendments in Appendices A and B, the proposed DSC amendments in Appendices C and D, the Standard in Appendix E and all related written comments received by the OEB will be available for public viewing on the OEB's website at www.oeb.ca.

If you have any questions regarding the proposed amendments described in this Notice, please contact Muzi Liu at Muzi.Liu@oeb.ca. The OEB's toll free number is 1-888-632-6273.

DATED at Toronto, **February 12, 2024**

ONTARIO ENERGY BOARD

Nancy Marconi

Digitally signed by Nancy Marconi
Date: 2024.02.12 13:54:50 -05'00'

Nancy Marconi
Registrar

Attachments:

Appendix A: Proposed Amendments to the Transmission System Code – Comparison Version to Current Code

Appendix B: Proposed Amendments to the Transmission System Code – Clean Version
Appendix C: Proposed Amendments to the Distribution System Code – Comparison Version to Current Code
Appendix D: Proposed Amendments to the Distribution System Code – Clean Version
Appendix E: Cyber Security Standard

Appendix A

to

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

February 12, 2024

EB-2023-0173

Proposed Amendments to the Transmission System Code – Comparison Version to Current Code

Note: Underlined text indicates proposed additions to the Transmission System Code. Numbered titles are included for convenience of reference only.

3B.2 Cyber Security

3B.2.1

"Cyber Security Standard" means the Cyber Security Standard document that was issued on [INSERT DATE], as updated from time to time.

3B.2.4 Compliance with the Cyber Security Standard

A transmitter shall comply with the Cyber Security Standard.

Appendix B

to

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

February 12, 2024

EB-2023-0173

Proposed Amendments to the Transmission System Code – Clean Version

3B.2 Cyber Security

3B.2.1 Definitions

"Cyber Security Standard" means the Cyber Security Standard document that was issued on [INSERT DATE], as updated from time to time.

3B.2.4 Compliance with the Cyber Security Standard

A transmitter shall comply with the Cyber Security Standard.

Appendix C

to

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

February 12, 2024

EB-2023-0173

Proposed Amendments to the Distribution System Code – Comparison Version to Current Code

Note: Underlined text indicates proposed additions to the Distribution System Code. Numbered titles are included for convenience of reference only.

1.2 Definitions

"Cyber Security Standard" means the Cyber Security Standard document that was issued on [INSERT DATE], as updated from time to time.

6.8.3 Compliance with the Cyber Security Standard

A distributor shall comply with the Cyber Security Standard.

Appendix D

to

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

February 12, 2024

EB-2023-0173

Proposed Amendments to the Distribution System Code – Clean Version

1.2 Definitions

"Cyber Security Standard" means the Cyber Security Standard document that was issued on [INSERT DATE], as updated from time to time.

6.8.3 Compliance with the Cyber Security Standard

A distributor shall comply with the Cyber Security Standard.

Appendix E

to

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

February 12, 2024

EB-2023-0173

Ontario Cyber Security Standard

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

Month dd, yyyy

Ontario Cyber Security Standard

Version 1.0

1. Purpose

The purpose of the Ontario Cyber Security Standard (Standard) is to enhance cyber security readiness of Ontario's electricity system. The provisions of the Standard are given force by requirements of section 3B.2.4 of the Transmission System Code (TSC) and section 6.8.3 of the Distribution System Code (DSC). Compliance with the TSC and DSC is a condition of the OEB's electricity transmitter and electricity distributor licences, respectively. Pursuant to the *Ontario Energy Board Act, 1998*, OEB codes, including the TSC and DSC, may incorporate by reference, in whole or in part, any standard, procedure or guideline. In case of any conflict between the Standard and the TSC or DSC, the provisions of the TSC or DSC, as applicable, shall govern.

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 Ontario Cyber Security Framework that was issued December 20, 2017, as amended from time to time.

"Lighthouse service" means the cyber security situational awareness and information sharing service provided by the Independent Electricity System Operator (IESO). At the time of coming into force of this definition, that service is named Lighthouse, but this term will be applicable to the service as it may be renamed from time to time.

"MIL" means Maturity Indicator Level and has the meaning ascribed to it in the Cyber Security Framework.

3. Participation in the IESO's Lighthouse Service

A transmitter or distributor shall participate in the IESO's Lighthouse service and will confirm its participation as required by the OEB. Participation will be evidenced by the transmitter or distributor:

a) having signed the participation agreement provided by the IESO

b) having been granted access to the Lighthouse Member Portal by the IESO

c) having established a secure network connection with the IESO's Lighthouse solution infrastructure

4. Cyber Security Framework

A transmitter or distributor shall implement the following Cyber Security Framework control objectives at MIL2 and report on their implementation:

a) ID.AM-6

b) ID.AM-P1, and 2

c) ID.GV-1, 2, 3, and 4

d) ID.GV-P1, P2, and P3

e) ID.RA-P1

f) PR.AT-4 and 5

g) ID.RM-1

h) ID.RM-P1