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

**BY EMAIL AND WEB POSTING**

March 27, 2024

**NOTICE OF AMENDMENTS TO CODES TO ENHANCE CYBER SECURITY READINESS**

**AMENDMENTS TO THE TRANSMISSION SYSTEM CODE AND THE DISTRIBUTION SYSTEM CODE**

**BOARD FILE NO.: EB- 2023-0173**

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

---

Given the potential for heightened cyber security risk as the energy transition proceeds and new technologies are integrated into Ontario's electricity system, the Ontario Energy Board (OEB) is giving notice under section 70.2 of the *Ontario Energy Board Act, 1998* (Act) of final amendments to the *Transmission System Code* (TSC) and the *Distribution System Code* (DSC). These amendments, which come into force on **October 1, 2024**, are intended to facilitate and enhance cyber security readiness, collaboration and innovation in Ontario's electricity sector.

Per the amendments, licensed electricity transmitters and distributors (utilities) will be required to comply with a new Ontario Cyber Security Standard document (Standard), which sets out specific cyber security readiness requirements.

## A. Background

On February 12, 2024, the OEB issued for comment a Notice of Proposal (February Notice) in which it proposed amendments (proposed amendments) to the TSC and DSC. The proposed amendments aimed to protect the public interest by enhancing utility resilience and reinforcing the OEB's monitoring of utility compliance with existing customer information security expectations.

The OEB invited written comments on the proposed amendments and received comments from one transmitter. In its comments, the transmitter supported the proposed amendments and provided specific comments on the proposed Standard.

Having considered the transmitter's comments and suggestions, the OEB applied minor revisions to the Standard, to clarify the OEB's expectations.

Final TSC amendments are set out in Appendices A (blackline relative to the existing TSC) and B (final text for TSC) of this notice.

Final DSC amendments are set out in Appendices C (blackline relative to the existing DSC) and D (final text for DSC) of this Notice.

**B. Adoption of February Proposed TSC and DSC Amendments**

In the February Notice, the OEB proposed a similar amendment to both section 3B.2.1 of the TSC and section 6.8.3 of the DSC.

The February Notice explained that section 3B.2.1 of the TSC and section 6.8.3 of the DSC 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 TSC or DSC and is not subject to the requirements of section 70.2 of the Act. Although it is not part of the TSC or DSC, the Standard is provided for information in Appendix E to this Notice.

As discussed in the February Notice, the Standard will allow the OEB 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 remains as set out in the TSC and DSC. Accessible to utilities as a key cyber security reference document, the Standard initially focuses on foundational elements to enhance and strengthen utility cyber security readiness. Specifically:

a) making participation in the Independent Electricity System Operator's Lighthouse information sharing and situational awareness service mandatory for all licensed transmitters and distributors; and
b) making specific governance and privacy related portions of the Ontario Cyber Security Framework mandatory for applicable transmitters and distributors.

The OEB expects that the situational awareness requirement will provide utilities with access to cyber security intelligence, tools and related products to improve utilities' resilience in the face of an ever-evolving cyber security threat landscape, and the privacy and governance requirements will reinforce the protection of personal information and organizational decision making, respectively.

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

## C. Anticipated Costs and Benefits

The anticipated costs and benefits associated with the proposed amendments were set out in the February Notice. Interested parties should refer to the February Notice for a detailed discussion in that regard.[2]

## D. Coming into Force

Recognizing the time that some utilities may need to comply, amendments to the TSC and DSC, as set out in Appendix A and Appendix C respectively, come into force on **October 1, 2024**. The OEB's approach to assessing ongoing compliance with the proposed amendments and the Standard was set out in the February Notice.

For transmitters' and distributors' reference, and because there are questions in the cyber security reports that are to be answered and submitted in April 2024 (as part of the OEB's *Reporting and Record Keeping Requirements* (RRR)) that align with certain requirements of the Standard, the OEB is repeating that text here:

> *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 OEB's Reporting and Record Keeping Requirements. 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.*

[2] February Notice, p.5.

If you have any questions regarding the code 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, March 27, 2024

**ONTARIO ENERGY BOARD**

Nancy Marconi

Digitally signed by Nancy Marconi
Date: 2024.03.27 13:50:53 -04'00'

Nancy Marconi
Registrar

Attachments:

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

**Appendix A**

**to**

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

**March 27, 2024**

**EB-2023-0173**

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

*Note: Underlined text indicates 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 March 27, 2024, 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 Amendments to the**
**Transmission System Code and the Distribution System Code**

**March 27, 2024**

**EB-2023-0173**

## 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 March 27, 2024, 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 Amendments to the**
**Transmission System Code and the Distribution System Code**

**March 27, 2024**

**EB-2023-0173**

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

*Note: Underlined text indicates 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 March 27, 2024, 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 Amendments to the**
**Transmission System Code and the Distribution System Code**

**March 27, 2024**

**EB-2023-0173**

## Amendments to the Distribution System Code – Clean Version

1.2 Definitions

…

"Cyber Security Standard" means the Cyber Security Standard document that was issued on March 27, 2024, 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 Amendments to the Transmission System Code and the Distribution System Code

**March 27, 2024**

**EB-2023-0173**

## Ontario Cyber Security Standard

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

# Ontario Cyber Security Standard

Version 1.0
Issue Date: March 27, 2024
Effective Date: October 1, 2024

## 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; and

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

## 4. Cyber Security Framework

4.1 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.GV-1, 2, 3, and 4

c) PR.AT-4 and 5

d) ID.RM-1

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

a) ID.AM-P1, and 2

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

c) ID.RA-P1

d) ID.RM-P1