Ontario | 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