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

Ontario Cyber Security Standard

Version 2.0

Original Issue Date: March 27, 2024
Original Effective Date: October 1, 2024
Version 2.0 Issue Date: December 16, 2024

TABLE OF CONTENTS

APPENDICES

1. Purpose

The purpose of the Ontario Cyber Security Standard (Standard) is to enhance the 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 Ontario Energy Board's (OEB) 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.

"Control Objective" means the subcategory in the Ontario Cyber Security Framework.

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

"Independent Assessment" means a cyber security assessment conducted by an independent assessor of a transmitter or distributor's MIL for each control objective.

"Independent Assessor" means a third-party individual, independent of a transmitter or distributor, that meets the minimum qualifications listed in the Standard, procured by a transmitter or distributor to conduct an independent assessment.

"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.

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

"NIST Cybersecurity Framework" means the National Institute of Standards and Technology's cyber security framework.

“Report” means the completed Independent Cyber Security Assessment Report, by an independent assessor, using the Reporting Template.

“Reporting Template” means the OEB’s Independent Cyber Security Assessment Report template which is provided in Appendix 1 of the Standard.

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

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

5. Independent Assessment

5.1 A transmitter or distributor shall obtain an Independent Assessment in accordance with the schedule determined, from time to time, by the OEB and comply with all of the following requirements:

a) A transmitter or distributor shall retain an Independent Assessor, with the following minimum qualifications, to conduct an Independent Assessment:

1. ten or more years of experience in conducting cyber security assessments, including experience with applying the NIST Cybersecurity Framework; and

2. must have completed three cyber security assessments, in the five years prior to conducting the Independent Assessment, including at least one such assessment for a Canadian electricity transmitter or distributor, Canadian public sector organization or Canadian government entity;

b) An Independent Assessor shall assess a transmitter or distributor's MIL for each control objective in the version of the Cyber Security Framework that is in effect twelve months before the reporting deadline established by the OEB for that transmitter or distributor, and complete the Reporting Template;

c) The Reporting Template shall be completed as follows:

(1) The Independent Assessor shall complete the following sections in the Reporting Template:

i. OCSF sub-category.

ii. Current state observation.

iii. Current state MIL.

iv. Applicability of current state MIL

v. Recommended actions (if applicable)

(2) The Independent Assessor shall sign and date the Report upon completion of the Independent Assessment. The Independent Assessor's signature on the Report shall be dated no earlier than six months before the reporting deadline established by the OEB.

d) A transmitter or distributor shall submit the completed Report to the OEB, on or before the reporting deadline established by the OEB.

5.2 Following the review of a transmitter's or distributor's Report, the OEB may require a transmitter or distributor to submit an action plan providing the steps the transmitter or distributor intends to take with respect to any recommendations contained in the Report, including any target MILs for specific Control Objectives and the timeline for achieving the target MILs and completing any other planned actions.

Appendix 1 – Reporting Template

ONTARIO ENERGY BOARD

Independent Cybersecurity Assessment Report

Name of Utility:		Date
Electronic Signature of Qualified Individual:		
Electronic Signature of Utility Representative:		

Independent Assessment Results (To be Completed by the Independent Assessor)					
#	**OCSF Subcategory** *(The subdivision of a Category into specific outcomes of technical and/or management activities)*	**Current State Observation** *(Present condition or status of a system or process)*	**Current State MIL** *(Indicates the current state maturity level of the entity's cyber security practices)*	**Applicability of Current State MIL** *(Indicates the applicability of the assessed Current State MIL based on the entity's cyber security risk level)*	**Recommended Actions** *(If Applicable)*