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

Ontario Cyber Security Standard

Version 3.1

Original Issue Date: March 27, 2024
Original Effective Date: October 1, 2024
Version 2.0 Issue Date: December 16, 2024
Version 3.0 Issue Date: August 20, 2025
Version 3.1 Issue Date: November 6, 2025

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.

"Cyber Security Incident" means a confirmed, intentional, successful, and unauthorized action to gain access to, modify, destroy, delete, or render unavailable information or any information technology or operating technology network or system that is owned, operated or used by the transmitter or distributor.

"Cyber Security Incident Report" means the completed Cyber Security Incident Report, prepared by a transmitter or distributor, using the Cyber Security Incident Report Template, submitted to the IESO by way of the Lighthouse Member Portal, email or another method prescribed by the IESO.

"Cyber Security Incident Report Template" means the Cyber Security Incident Report Template which is provided in Appendix 2 of this Standard.

"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.

"IESO" means the Independent Electricity System Operator.

"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.

“Independent Cyber Security Assessment Report” means the completed Independent Cyber Security Assessment Report, prepared by an independent assessor, using the Independent Cyber Security Assessment Report Template, and signed and dated by an Independent Assessor and the Chief Executive Officer of the transmitter or distributor.

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

“Lighthouse service” means the cyber security situational awareness and information sharing service provided by the 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.

“Notable Cyber Security Incident Report” means a Cyber Security Incident Report that is determined to be a Notable Cyber Security Incident Report when a transmitter or distributor responds affirmatively to one or more of the following questions on the Cyber Security Incident Report:

i) Has the incident caused, or is it likely to cause, a disruption, degradation, or other negative impact in the reporting entity’s ability to reliably transmit or distribute electricity?

ii) Has the incident caused, or is it likely to cause, a disruption, degradation, or other negative impact to quality of service provided to customers of the reporting entity?

iii) Other than the IESO, has the incident been, or will it be, reported to the Ontario Government, a news media agency, or to the reporting entity’s customers?

iv) Has the incident resulted in, or is likely to result in, the disclosure of customer information to any third party, except where the customer has provided prior written consent?

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 Independent Cyber Security Assessment Report Template;

c) The Independent Cyber Security Assessment Report Template shall be completed as follows:

(1) The Independent Assessor shall complete the following sections in the Independent Cyber Security Assessment Report 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 and the transmitter's or distributor's Chief Executive Officer shall sign and date the Independent Cyber Security Assessment Report upon completion of the Independent Assessment. The Independent Assessor's signature on the Independent Cyber Security Assessment 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 Independent Cyber Security Assessment Report to the OEB signed by its Chief Executive Officer, on or before the reporting deadline established by the OEB.

5.2 Following the review of a transmitter's or distributor's Independent Cyber Security Assessment 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 Independent Cyber Security Assessment Report, including any target MILs for specific Control Objectives and the timeline for achieving the target MILs and completing any other planned actions.

6. Cyber Security Incident Reporting

6.1 A transmitter or distributor shall notify the IESO of a Cyber Security Incident involving the transmitter or distributor by submitting a Cyber Security Incident Report to the IESO by the end of the next business day following the confirmation that a Cyber Security Incident has occurred.

6.2 A transmitter or distributor shall complete the four questions that determine whether a Cyber Security Incident Report is a Notable Cyber Security Incident Report. Notable Cyber Security Incident Reports will be shared with the OEB by the IESO in accordance with its licence requirements.

6.3 Where a transmitter or distributor becomes aware of new information that materially alters the content of a previously submitted Cyber Security Incident Report, the transmitter or distributor shall submit a revised Cyber Security Incident Report to the IESO by the end of the next business day following the receipt of the new information.

6.4 A transmitter or distributor shall respond to an information request by the IESO or OEB related to a Cyber Security Incident, including but not limited to the organization’s security controls, processes and risks, and shall provide the requested information, within the timeline stated by the IESO or OEB at the time of the request.

Appendix 1 – Independent Cyber Security Assessment Report Template

Independent Cyber Security Assessment Report

Name of Transmitter or Distributor:		**Date**
Electronic Signature of Independent Assessor:		
Electronic Signature of Chief Executive Officer:		

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)*

Appendix 2 – Cyber Security Incident Report Template

CYBER SECURITY INCIDENT:

A confirmed, intentional, successful, and unauthorized action to gain access to, modify, destroy, delete, or render unavailable information or any information technology or operating technology network or system that is owned, operated or used by the transmitter or distributor.

Please complete the following sections to the best of your knowledge at the time of submission. Text in gray provides details on the content for a section and can be removed prior to submission.

Incident Details

Name of Reporting Entity:

Name of Impacted Licensed Ontario Transmission or Distribution Entity if Different From Above:

Date and Time Incident Occurred:		Date and Time Incident Confirmed:	

Type of Cyber Security Incident:

Examples include Social Engineer/Phishing, Denial of Service, Vulnerability Exploitation, Malware/Ransomware, Brute Force or Password Attack, Code/SQL Injection, Attacker-in-the-middle, Insider Threat, Supply Chain Attack, Data Breach.

Impact:

What were the impact(s) of the cyber security incident? Examples include the installation of Malware or Ransomware, Loss/Breach of data, Service Disruption, Service Degradation, or Fraud.

Description of the Cyber Security Incident:

Include, where known, the initial attack vector, root cause, activities performed in response to the incident, and planned remediation activities that have not been completed.

Cyber Security Incident Status:

Under investigation, Active Remediation, Active Recovery, Resolved

Indicators of Compromise (IOC):

Indicators of compromise (IOCs) are evidence or artifacts observed on a network or a technology asset that indicate malicious or suspicious activity. Typical IoCs include IP addresses, file hashes, urls or domain names, and bash/powershell commands observed during a cyber security incident. IoCs can also include anomalous activities or behaviours such as unknown applications, irregular privileged user account activity, unusual network traffic patterns, and unauthorized system changes.

Incidents that will be reported to the OEB

The IESO will forward this incident report to the OEB if the response to one or more of four questions in the following section is 'Yes'

Has the incident caused, or is it likely to cause, a disruption, degradation, or other negative impact in the reporting entity's ability to reliably transmit or distribute electricity?

☐Yes ☐ No

If yes, what is the nature of the disruption, degradation, or negative impact?

Has the incident caused, or is it likely to cause, a disruption, degradation, or other negative impact in quality of service provided to customers of the reporting entity?

☐Yes ☐ No

If yes, what is the nature of the disruption, degradation, or negative impact?

Other than the IESO, has this incident been, or will it be, reported to the Ontario Ministry of Energy and Mining, a news media agency, or to the reporting entity's customers?

☐Yes ☐ No

Has the incident resulted in, or is likely to result in, the disclosure of customer information to any third party, except where the customer has provided prior written consent?

☐Yes ☐ No

Other than the IESO, who has this incident been, or will it be, reported to?

Including, but not limited to, law enforcement; municipal, provincial, or federal agencies such as the Ontario Ministry of Energy and Mining or Canadian Centre for Cyber Security; Service providers such as insurance or I.T. Managed Service Provider; news media; and customers?

Contact Information

Please provide contact details that will be used for any follow up requests for information	
Contact's Name:	Contact's Title:
Contact's Email:	Contact's Telephone Number:
This form is to be submitted to the IESO through the Lighthouse Portal or sent to the email address cybersecurity@ieso.ca by the end of next business day following the determination that a confirmed cyber security incident has occurred. When new information is identified by the reporting entity that changes the report content or responses the reporting entity is required to update the IESO through the Lighthouse Portal or sent to the email address cybersecurity@ieso.ca by the end of the next business day.	