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

BY EMAIL AND WEB POSTING

February 12, 2024

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

Re: Utility Cyber Security Reporting Changes

Ahead of the April 2024 filing timeline, the Ontario Energy Board (OEB) is making changes to improve the effectiveness of the cyber security reports that are part of the Reporting and Record-keeping Requirements (RRR) for licensed electricity distributors and transmitters (utilities). The objectives of the changes are to:

- clarify which specific Ontario Cyber Security Framework (OCSF) control actions utilities should be evaluating when responding to each question;
- increase the granularity of response options for utilities;
- enable utilities to report against OCSF version 1.1 that was released in December 2023; and,
- promote ongoing cyber security risk reduction and continuous improvement.

The OEB is also creating a confidential, risk-appropriate benchmarking tool that will be made available to utilities through the reporting portal in mid-2024.

Background

Since 2018, the OEB has been receiving reports on cyber security readiness from utilities as part of its RRR. These reports provide information on each entity's implementation of the OCSF.

On February 7, 2023, OEB staff issued a letter describing, among other things, changes to the RRR cyber security report that adopt utilities' suggestions to make the reporting more effective. With these changes, the report will better reflect that cyber security risk reduction is an ongoing activity, and that continuous improvement of systems and processes are necessary to maintain cyber security readiness.

The changes also create clearer alignment between the cyber security report questions and the OCSF. The OCSF is maintained and advanced by the Cyber Security Advisory Committee (CSAC), an industry-led group comprised of utility representatives and other stakeholders. Over the course of 2023, OEB staff engaged with the CSAC about these improvements, and the CSAC has meaningfully contributed to the revision process. In December 2023, the CSAC released version 1.1 of the OCSF. This version added several new control actions and more illustrative examples to guide utility evaluation.

Furthermore, the letter also described the OEB's plan to act on requests by senior utility leaders for a benchmarking tool that will help them understand how their individual cyber security report responses compare with those of other utilities. Beginning in mid-2024, a confidential risk-appropriate benchmarking tool will be made available to utilities through the RRR portal. This tool will aggregate the cyber security report responses of the low, medium and high-risk utilities, respectively, and display them in an anonymized format. This tool will be updated annually, after the April 2024 RRR submission.

The changes to the RRR cyber security report are summarized in the following table. The new RRR cyber security report can be found in Appendix A.

Objectives	**Changes**
Clarify which specific OCSF control actions utilities should be evaluating when responding to each question	Map relevant OCSF control actions to each of the 11 cyber security report questions. Control objectives that have been introduced in version 1.1 of the OCSF have been identified with an asterisk.
Increase the granularity of response options	Modified response options for several questions to put utilities' implementation of the OCSF on a percentage scale (0-25%, 26-49%, etc.)
Enable utilities to report against OCSF version 1.1	Utilities will have the option of reporting against OCSF version 1, or version 1.1
Facilitate utility benchmarking	A risk-appropriate benchmarking tool will be made available in mid-2024

Any questions relating to this letter should be directed to Muzi Liu, Senior Advisor at muzi.liu@oeb.ca. The OEB's toll-free number is 1-888-632-6273.

Yours truly,

Brian Hewson
Vice President
Consumer Protection & Industry Compliance

Attachment:
Appendix A – Cyber Security Readiness Report

Appendix A:

Cyber Security

Readiness Report

All information submitted in this process will be kept confidential and used by the OEB solely for the purpose of assessing the industry's cyber security readiness.

PART 1 – GENERAL INFORMATION

Licensee Name:	
Licensee ID:	
Cyber Security Contact Name:[1]	
Cyber Security Contact Telephone No.:	
Cyber Security Contact E-mail:	

Self-Certification Statement: I attest to the reported cyber security readiness outlined in this report for the licensee as of the report completion date.

Chief Executive Officer (CEO) Name:	
CEO Signature:	
Date CEO Signed:	

PART 2 – REQUEST FOR INFORMATION

Pursuant to the "*Electricity Reporting and Record Keeping Requirements*", licensees are required to provide the OEB with information on cyber security readiness and actions they are taking relative to their cyber security risks. Using the Ontario Cyber Security Framework (Framework), licensees shall identify the control objectives that would apply to their organization in accordance with their Inherent Risk Profile.

Licensees are expected to determine the control objectives that they plan to implement and how they will be achieved based upon their assessment of their organization's cyber security risk tolerance. This information is to be provided by completing Part 3 and Part 4 of this form.

[1] Cyber Security Contact Name is the individual at your organization who would be contacted about a cyber security update.

PART 3 - ACKNOWLEDGEMENT OF STATUS

Signatory(s) confirms:

I have read and understand the Framework and in applying the self-assessment steps using the Inherent Risk Profile Tool, my organization's risk would be rated as:	□ HIGH □ MEDIUM □ LOW

Licensees to select one check box □ in the categories 'Some', 'All', or 'Exceed' based on your risk profile, as identified using the Inherent Risk Profile Tool.

PART 4 - SUPPORTING INFORMATION – CYBER SECURITY

STATUS OF IMPLEMENTATION OF CONTROL OBJECTIVES CONSISTENT WITH MY ORGANIZATION'S RISK PROFILE.		
PLANS TO IMPLEMENT **SOME** CONTROL OBJECTIVES	□	Control objectives critical to my organization are implemented.
	□	Control objectives critical to my organization are planned to be implemented within __ years.
PLANS TO IMPLEMENT **ALL** CONTROL OBJECTIVES	□	Control objectives defined in the Framework are implemented.
	□	Control objectives defined in the Framework are planned to be implemented in __ years.
PLANS TO **EXCEED** CONTROL OBJECTIVES	□	Additional control objectives critical to my organization have been implemented.
	□	Additional control objectives critical to my organization are planned to be implemented in __ years.

Please answer the following questions by selecting from the dropdown list that most closely reflects your efforts, considering the associated Ontario Cyber Security Framework control objectives. Status report for the period from January 1, 2023 to December 31, 2023:

*Please specify the version of the Ontario Cyber Security Framework to which your organization is referring to. Control objectives marked with an asterisk (*) have been introduced in version 1.1 of the Framework:

- V1.0
- V1.1

1. a) Does your organization have a corporate privacy and cyber security governance program[2] in place?	• Yes • No
1. b) Is the utility's board of directors involved in the cyber security risk management process?	• Yes • No
Question 1 related control objectives:	
IDENTIFY	**PROTECT**
ID.AM-6 ID.AM-P1, 2 ID.GV-1, 2, 3 ID.GV-P1, P2 ID.RA-P1	PR.AT-4, 5

2. a) Based on your organization's risk profile, do you have privacy and cyber security risk identification and risk prioritization processes in place to support your operational risk decisions?	• Yes • No
Question 2 a) related control objectives:	
IDENTIFY	
ID.RM-1 ID.RM-P1 ID.GV-P3 ID.GV-4	

[2] Effective Information Security Governance Program NIST SP 800-100 p.14

2. b) Based on your organization’s risk profile, does your organization have privacy and cyber security risk identification and risk prioritization processes in place to support your operational risk decisions? What is the level of completion?	• Not Implemented • 1 to 25% • 26 to 50% • 51 to 75% • 76 to 100%
Question 2 b) related control objectives:	
IDENTIFY	
ID.RA-1, 2, 3, 4, 5, 6 ID.RM- 2, 3	

3. a) Does your organization undergo 3rd party and/or self-audits /assessments[3] of your privacy and cyber security program based on your organization’s risk profile?	**3rd Party Audits/Assessments:** • Yes • No **Self-Audits/Assessments:** • Yes • No
3.b) Does your organization have mitigation plans in place for your organization’s privacy and cyber security risk areas based on your 3rd party or self-assessment? What is the level of completion?	• Not Implemented • 1 to 25% • 26 to 50% • 51 to 75% • 76 to 100%
Question 3 related control objectives:	
IDENTIFY	**PROTECT**
ID.RA-1 ID.RA-6	PR.IP-12

4. a) Has your organization completed its onboarding into the IESO Information Sharing Services program known as Lighthouse? (Note: If you are unsure of your status please contact the IESO for confirmation.)	• Yes • In progress • No

[3] Ontario Cyber Security Framework, Auditing p.18

4. b) For those organizations that have completed onboarding into the IESO's Lighthouse program, do you actively participate in one or more of the IESO's information sharing services?	**Cyber Security Situational Awareness** □ Actively Using Information □ Not Using Information **Information exchange** □ Actively Participating □ Not Participating
Question 4 related control objectives:	
IDENTIFY	**RESPOND**
ID.RA-2	RS.AN-5*

5. Does your organization have a privacy and cyber security awareness education and training program in place for the organization's personnel and partners to perform their information security-related duties and responsibilities consistent with related policies, procedures, standards, and agreements?[4] What is the level of completion?	• Not Implemented • 1 to 25% • 26 to 50% • 51 to 75% • 76 to 100%
Question 5 related control objectives:	
PROTECT	
PR.AT-1, 2, 3, 4, 5 PR.AT-P1	

[4] NIST Privacy Security Controls Self-Assessment Questionnaire

6. Does your organization have controls in place to address privacy and cyber security for 3rd party service providers? What is the level of completion?

- Not Implemented
- 1 to 25%
- 26 to 50%
- 51 to 75%
- 76 to 100%

Question 6 related control objectives:

IDENTIFY	PROTECT	RESPOND
ID.AM-6 ID.GV-2 ID.SC-1*, 2*, 3*, 4*, 5*	PR.AT-3	RS.CO-4 RS.AN-5*

7. Does your organization have systems and/or processes in place to identify, protect and detect cyber security and privacy events/incidents?[5] What is the level of completion?

- Not Implemented
- 1 to 25%
- 26 to 50%
- 51 to 75%
- 76 to 100%

Question 7 related control objectives:

IDENTIFY	PROTECT	DETECT	RESPOND
ID.RA-2, 3, 4, 5, 6	PR.AC-1, 2, 3, 4, 5 PR.DS-1, 2, 3, 4, 5, 6, 7 PR.PT-1, 2, 3, 4 PR.AC-6*, 7* PR.DS-8* PR.PT-5*	DE.AE-1, 2, 3, 4, 5 DE.CM-1, 2, 3, 4, 5, 6, 7, 8	RS.AN-1, 2, 3

[5] NISTR – 72.98r2 p.57 “actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.”
NIST SP800-61r2 p.6 Cyber Security Incident Handing Guide “computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

8. Does your organization have documented incident response processes and procedures in place for privacy and cyber security events/incidents? What is the level of completion?	• Not Implemented • 1 to 25% • 26 to 50% • 51 to 75% • 76 to 100%
Question 8 related control objectives:	
PROTECT	**RESPOND**
PR.IP-9	RS.RP-1 RS.CO-1, 2, 3, 4, 5 RS.AN-4 RS.MI-1, 2, 3

9. Are you regularly testing your documented event/incident response processes and procedures for privacy and cyber security?	• Yes • No
Question 9 related control objectives:	
PROTECT	**RESPOND**
PR.IP-10	RS.IM-1, 2

10. Does your organization have documented incident recovery processes and procedures in place for privacy and cyber security events/incidents? What is the level of completion?	• Not Implemented • 1 to 25% • 26 to 50% • 51 to 75% • 76 to 100%
Question 10 related control objectives:	
PROTECT	**RECOVER**
PR.IP-9	RC.RP-1

11. Are you regularly testing your documented event/incident recovery processes and procedures for privacy and cyber security?	• Yes • No
Question 11 related control objectives:	
PROTECT	**RECOVER**
PR.IP-10	RC.IM-1, 2