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

BY EMAIL AND WEB POSTING

February 7, 2023

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

Re: Enhancing Cyber Security Readiness in Ontario's Electricity Sector

In its 2022-23 Business Plan the Ontario Energy Board (OEB) identified the increasing threat of cyber security risks to the electricity sector, as well as the importance of the industry acting to address these risks particularly in light of the energy transition and new technologies being adopted in the sector. To get started, in September and October 2022, OEB staff met with senior leaders representing 54 licensed electricity distributors to understand the challenges and opportunities to enhance cyber security readiness in Ontario's electricity sector. The OEB appreciates distributors' participation in these productive discussions. This letter summarizes what we heard from distributors and sets out the OEB's proposed actions to enhance cyber security readiness in the sector.

On October 21, 2022, the Minister of Energy provided the OEB with a renewed Letter of Direction that updated the Minister's expectations for the OEB in the upcoming three-year business planning period. The Letter of Direction stated that the OEB has an important role to play in ensuring that distributors are preparing the distribution system to mitigate reliability and resiliency risks. The Letter of Direction included distributor collaboration on cyber security as one means of enabling cost-effective distribution system reliability and resiliency. A number of the actions we are planning to take rely on collaboration across the sector aligning with both what we heard from distributors and the direction in the Minister's letter.

The Regulatory Framework for Cyber Security

Licensed distributors and transmitters (utilities) are responsible for cyber security risk management as part of their overall business risk and are accountable for making the appropriate investments to mitigate those risks. The OEB's role is to set the

expectations for the utilities in terms of managing risks as part of their responsibility for providing consumers with reliable service.

In 2018, the Cyber Security Advisory Committee (CSAC), an industry-led committee consisting of representatives of Ontario's electricity utilities and other stakeholders, was established. The purpose of the CSAC is to provide the OEB with expert advice and to evolve Ontario's Cyber Security Framework (OCSF), which has been in place since 2017, guided by changes in the cyber security landscape and industry best practices. The voluntary OCSF recommends a set of control objectives for a utility to implement based on its risk profile. The OEB anticipates that the CSAC will produce the next version of the OCSF in 2023. The OEB appreciates the time and effort contributed by utility representatives to participate in and lead this important industry forum.

The Independent Electricity System Operator (IESO) is licenced to provide and promote centralized Cyber Security Information Sharing (CSIS) services accessible to all distributors and transmitters. In 2019, the IESO launched Lighthouse, the main component of the IESO's cyber security sector services offering. Lighthouse is a situational awareness and information-sharing service for participating utilities.

The changes in the electricity system associated with the energy transition, including the use of emerging technologies, will make the electricity system more complex and more vulnerable to cyber attacks. Since 2018, utilities have been required to report annually to the OEB on the status of cyber security readiness as part of the reporting and record keeping requirements (RRR). These reports provide information regarding each entity's implementation of the OCSF. Analysis of this reporting has identified areas for potential improvement in the context of the changing risk environment and has led to this initiative to enhance cyber security readiness in the electricity sector.

Challenges and Opportunities Identified by Distributors

Distributors described several underlying challenges associated with cyber security and the OCSF. First, continuous investment is required to keep up with constantly changing cyber security risks and emerging technologies. Second, cyber security risks span across information technology and operating technology and different security tools are required for each. Finally, governance components of the OCSF – which are policy, process and structure based – are some of the most challenging to implement.

Distributors also provided the following observations:

- CSAC has the potential to lead the improvement of Ontario's electricity sector cyber posture by evolving the OCSF and maintaining close relationships with the OEB and the IESO

- Lighthouse is a valuable program that will be most effective if all transmitters and distributors participate
- Utilities would like to be able to benchmark their cyber security readiness compared to their peers
- The OEB should work with the CSAC to improve and clarify the cyber security RRR reporting questions
- While there is considerable sharing of knowledge amongst members of some utility industry groups, expanded information and resource sharing could help utilities make more efficient investments and manage costs

The OEB's Proposed Approach

OEB staff has considered the input from distributors and the direction from the Minister of Energy and identified a set of potential actions to support utilities in enhancing their cyber security readiness. These include opportunities for collaboration in the sector that will strengthen cyber readiness while ensuring cost effectiveness.

OEB staff views the CSAC as the primary forum for engaging with utilities on cyber security. The CSAC is also a vehicle for utilities to share innovative approaches to mitigating risks and to collaborate on solutions. OEB staff will continue to support the CSAC's efforts to improve and strengthen the OCSF.

OEB staff intends to have an ongoing dialog with utilities and the IESO principally through the CSAC. OEB staff expects that these discussions will be framed by the regulatory challenges and opportunities described above and will result in confirming specific OEB actions. OEB staff's potential options to enhance cyber security readiness include:

- Making the implementation of the OCSF's corporate privacy and cyber security governance control objectives mandatory for applicable utilities
- Making participation in the IESO's Lighthouse program mandatory for all transmitters and distributors
- Making changes to the OEB's RRR to address the issue raised by distributors that reporting should capture the continuous improvement of systems and processes necessary to maintain cyber readiness and align with OCSF implementation
- Assessing the feasibility of providing benchmarking information to utilities to track OCSF implementation, support collaboration and identify top performers

As described in the Appendix to this letter, OEB staff expects to work directly with the CSAC to refine these and other options and develop implementation plans. For

example, CSAC input will be critical to efficiently developing regulatory changes that are aligned with the upcoming version of the OCSF. Any specific regulatory requirements will go through the necessary consultation processes.

All licensed electricity transmitters and distributors are encouraged to participate in the CSAC. Please contact Muzi Liu, Senior Advisor at muzi.liu@oeb.ca with questions about this letter or for more information about CSAC participation.

Yours truly,

Brian Hewson
Vice President, Consumer Protection & Industry Performance

Appendix: Implementation Plan for Potential Actions

Potential OEB Action	Approach	Target Completion Date
Make changes to the OEB's RRR to align reporting requirements with the OCSF and increase the effectiveness of reporting	Consult with the industry (CSAC) on specific RRR changes	Changes implemented in time for 2023 annual reporting, which will occur in Q2 2024
Develop confidential and risk appropriate reporting on the sector's cyber security readiness to facilitate utility benchmarking	Consult with the industry (CSAC) and other stakeholders on an effective benchmarking design	By end of Q3 2024
Mandate the use of the OCSF's corporate privacy and cyber security governance control objectives for applicable utilities	Consult with the industry (CSAC) to develop an implementation plan for new OCSF requirements	By the end of Q3 2023
Mandate participation in the IESO's Lighthouse program for all licensed transmitters and distributors	Consult with the IESO and utilities that have not yet signed up for Lighthouse to understand the barriers for entry and address them by working closely with the entities	By the end of Q3 2023