



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

BY EMAIL

September 21, 2021

Ms. Christine E. Long  
Registrar  
Ontario Energy Board  
2300 Yonge Street, 27<sup>th</sup> Floor  
Toronto, ON M4P 1E4  
[Registrar@oeb.ca](mailto:Registrar@oeb.ca)

Dear Ms. Long:

**Re: Ontario Energy Board (OEB) Staff Submission on Confidentiality  
Independent Electricity System Operator  
Application for approval of 2020 and 2021 revenue requirement,  
expenditures and fees  
OEB File Number: EB-2020-0230**

---

In accordance with Procedural Order No. 3, please find attached the OEB staff submission for the above proceeding. This document has been sent to the Independent Electricity System Operator and to all other registered parties to this proceeding.

Yours truly,

*Original Signed By*

Andrew Bishop  
Project Advisor, Generation & Transmission

Encl.

cc: All parties in EB-2020-0230



# **ONTARIO ENERGY BOARD**

## **OEB Staff Submission on Confidentiality**

**Independent Electricity System Operator**

**Application for approval of 2020 and 2021 revenue requirement,  
expenditures and fees**

**EB-2020-0230**

**September 21, 2021**

## Background

The Independent Electricity System Operator (IESO) filed an application with the Ontario Energy Board (OEB) on May 27, 2021 under section 25(1) of the *Electricity Act, 1998*, seeking approval for its 2020 and 2021 expenditures, revenue requirement and fees.

In accordance with Procedural Order No. 2, OEB staff and intervenors filed interrogatories on or before August 19, 2021 and the IESO responded to interrogatories on September 9, 2021. As part of its response, the IESO requested confidential treatment of the unredacted attachments provided in response to the following School Energy Coalition (SEC) interrogatories: 1.5-SEC-15, 1.5-SEC-16, 1.5-SEC-17, and 1.5-SEC-18.1 The IESO stated that, for the following reasons, the information should be not be disclosed:

The attachments were developed as internal documents and contain information that is not the relevant business case information expected by the OEB's Decision and Order to EB-2019-0002 and as provided for in the IESO's application. As noted above, in an effort to be of assistance to the parties, the IESO is filing the attachments but requests that the redacted portions in the attachments be protected because its disclosure relates to public security. Disclosing information that relates to the IESO's IT systems creates a cyber security risk which would allow for a threat actor to gain insights into IESO systems and status that could be used for malicious purposes. As well, disclosing the names of individuals and detailed document IDs, or other identifiers, provide specifics that would enhance attacks against the IESO, such as phishing and impersonation attacks, that would allow a threat actor to obtain sensitive information. The IESO notes that the items that have been redacted from the documents that are the subject of this confidentiality request, have no bearing to the consideration of any issues in this proceeding.

Through Procedural Order No. 3 (PO), issued on September 14, 2021, the OEB allowed parties to file objections to the IESO's confidentiality request and for the IESO to reply to any objection, in accordance with the OEB's *Practice Direction on Confidential Filings* (Practice Direction). The PO provided that any objections are to be filed with the OEB and served on all parties by September 21, 2021 and the IESO's response to any objections is to be filed by September 23, 2021.

## OEB Staff Submission

OEB staff does not object to the IESO's request for confidential treatment of the unredacted attachments provided in response to the aforementioned SEC interrogatories. OEB staff is of the view that the information is sensitive and is not the type of information that is normally publicly available. OEB staff accepts the IESO's assertion that the information could create a cyber security risk and that the disclosure of the names of individuals and detailed document IDs have the potential to enhance attacks against the IESO, such as phishing and impersonation attacks.

OEB staff suggests that this type of confidential information is generally protected from public disclosure by the OEB. Among the OEB's considerations in determining requests for confidentiality set out in Appendix A of the Practice Direction is "the potential harm that could result from the disclosure of the information, including... whether the information pertains to public security...".<sup>1</sup>

~All of which is respectfully submitted~

---

<sup>1</sup> OEB Practice Direction on Confidential Filings, Appendix A, Clause (c)