

Toronto

Montréal

Calgary

Ottawa

Vancouver

New York

August 20, 2025

Adam Kardash
Direct Dial: 416.862.4703
akardash@osler.com
Our Matter Number: 1268459

Sent by Email

Nova Scotia Energy Board
3rd Floor, 1601 Lower Water Street
Halifax, Nova Scotia B3J 3P6

Attention: Crystal Henwood, Clerk of the Board

Dear Ms. Henwood:

M12273 – Inquiry of the Nova Scotia Energy Board (the Board) into Cybersecurity Incident of Nova Scotia Power (NS Power)

Thank you for your correspondence dated August 12, 2025. On behalf of our client, we reiterate that NS Power remains committed to working collaboratively and cooperatively with the Board to ensure that the Board receives all information needed for the Inquiry. We also thank the Board for the further information in your letter setting out the nature of the Inquiry and matters of concern to the Board.

A. Clarification of the Procedural Order Sought

NS Power understands that the Board applies the “open courts” principle, which allows for proportionate, public interest-based exceptions.¹ Our client appreciates the Board’s recognition that some of the information likely to be exchanged in this matter will be quite sensitive and require particularly strict confidentiality protection, and may warrant that it be provided only to the Board and no other parties in the proceeding.

Investigations into cybersecurity incidents generally occur within the proportionate exceptions to the “open courts” principle. By default, information received by regulatory authorities during an investigation of a cybersecurity incident is treated as confidential, including documents filed by parties. Disclosure is allowed in limited circumstances, including as part of the regulatory authority’s published report of findings. This is the nature of privacy regulatory authorities’ investigatory procedures referenced in paragraph 4(b) and footnote 1 of NS Power’s letter of August 8, 2025. Given privacy regulatory authorities’ extensive experience investigating cybersecurity incidents, we view their investigative procedures as being helpful and informative to the Board as it determines the

¹ *Sherman Estate v. Donovan*, 2021 SCC 25, at para 38.

process it will adopt for this matter. Excerpts of sample statutory provisions under Canadian and foreign privacy legislation are attached as **Appendix A**.

At the same time, NS Power expects that the Board will review claims of confidentiality throughout the Inquiry and will not automatically approve those claims without appropriate scrutiny.² To the extent that the Board has questions about NS Power's claims and rationale for confidentiality, NS Power respectfully requests the opportunity to further explain to the Board why it is necessary to hold the designated information in confidence, including, if necessary, through an oral hearing with the assistance of cybersecurity experts.

NS Power appreciates the Board will work with technical and professional advisors, including MNP Digital, to support its regulatory function. It was not NS Power's intention to prevent the Board from disclosing "Board Confidential" information to the Board's advisors. NS Power appreciates the point in your letter that the Board will consider the sensitive nature of the information in accessing its internal resources and external advisors, and assumes that any such external advisors will execute a confidentiality undertaking prior to their receipt of such confidential data.

Similarly, NS Power is assuming that all Intervenors in the Inquiry will execute a confidentiality undertaking prior to receiving any confidential data, as per the Board's normal process. Given the unique circumstances applicable to this cybersecurity incident, NS Power will have concerns regarding the highly sensitive nature of certain confidential data being disclosed in this proceeding, and, in relation to such information, will provide the appropriate justification to explain to the Board why it is necessary for the Board to hold such information in strict confidence and/or seek additional assurance as to the manner in which the information would be protected under a confidentiality undertaking, including the systems and protections that will be in place to safeguard this information.

Regarding the Board's requests for information issued on July 24, 2025 (the **IRs**), NS Power appreciates the extension granted by the Board on August 15, 2025, permitting the responses to be delivered on or before September 5, 2025. NS Power will endeavor to prioritize its efforts to respond to the IRs earlier than September 5, 2025, if possible.

NS Power also confirms that it will provide monthly progress reports regarding the Company's continuing response to the incident, and progress on the Incident Report requested by the Board. The Company will be sending the initial progress report to the Board today under separate cover. NS Power confirms that it will be in a position to file the Incident Report no later than December 31, 2025 (as required in your letter, dated July 14, 2025), and will endeavour to complete and submit the report earlier, if possible.

² Consistent with Rule 12 of the *Board Regulatory Rules*.

B. Request for Confidentiality

Further to the Board's request, attached to this letter as **Appendix B** are detailed reasons why NS Power's confidential submission of August 8, 2025 (the **Confidential Submission**) should be held in confidence by the Board. NS Power requests that Appendix B be held in confidence by the Board pursuant to Rule 12(2) of the *Board Regulatory Rules*. That said, NS Power is prepared to consent to the Board disclosing Appendix B and the Confidential Submission to the Intervenor to whom the Board has already granted standing, pursuant to the Board's normal process of requiring a confidentiality undertaking.

NS Power would be pleased to provide any further information that may assist the Board. We reiterate NS Power's commitment to working cooperatively and collaboratively with the Board throughout the Inquiry.

Sincerely,



Adam Kardash
Partner and Co-Chair, Privacy and Data Management, *Osler*

- c. W. David Rankin, *Osler*
Judith Ferguson, Executive Vice President, Regulatory, Legal, and Government
Relations, *Nova Scotia Power*

Appendix “A”

Statutory Excerpts

Federal: [*Personal Information Protection and Electronic Documents Act \(PIPEDA\)*, SC 2000, c 5, ss. 20\(1\) -\(1.1\)](#)

Confidentiality

20 (1) Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner’s duties or powers under this Part other than those referred to in subsection 10.1(1) or 10.3(2).

Confidentiality — reports and records

(1.1.) Subject to subsections (2) to (7), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information contained in a report made under subsection 10.1(1) or in a record obtained under subsection 10.3(2).

* * *

British Columbia: [*Personal Information Protection Act \(PIPA BC\)*, SBC 2003, c 63, s. 41\(1\)](#)

Restrictions on disclosure of information by commissioner and staff

41 (1) The commissioner and anyone acting for or under the direction of the commissioner must not disclose any information obtained in performing their duties or exercising their powers and functions under this Act, except as provided in subsections (2) to (6).

* * *

Alberta: [*Personal Information Protection Act \(PIPA Alberta\)*, SA 2003, c P-6.5, s. 41\(1\)](#)

Restrictions on disclosure of information

41 (1) The Commissioner and anyone acting for or under the direction of the Commissioner shall not disclose any information obtained in performing their duties, powers and functions under this Act, except as provided in subsections (2) to (4).

* * *

United Kingdom: [Data Protection Act 2018, \(ICO Data Protection Act\) UK Public General Acts, 2018 c. 12, s. 132\(1\)](#)

Confidentiality of information

132 (1) A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—

(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

(b) relates to an identified or identifiable individual or business, and

(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources,

unless the disclosure is made with lawful authority.

* * *

France: [Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés \(French Data Protection Act\), Chapter II, Article 11](#)

Art. II Les agents de la commission sont astreints au secret pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, sous peine des sanctions prévues à l'article 413-10 du code pénal et, sous réserve de ce qui est nécessaire à l'établissement du rapport annuel, à l'article 226-13 du même code.

Unofficial Translation

Art II The commission's agents are bound to secrecy with regard to facts, acts or information of which they may have become aware by reason of their functions, under penalty of the sanctions provided for in Article 413-10 of the Penal Code and, subject to what is necessary for the establishment of the annual report, in Article 226-13 of the same Code.

* * *

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

OSLER

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]