Nova Scotia Energy Board

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

Mailing Address
PO Box 1692, Unit M
Halifax, Nova Scotia B3J 3S3

TEL 902-424-1332
FAX 902-424-3919
TF 1-833-809-0040

board@novascotia.ca
nserbt.ca/nseb

September 17, 2025

Judith Ferguson
Executive Vice President, Regulatory,
Legal and Government Relations
Nova Scotia Power Incorporated
P.O. Box 910, 1223 Lower Water Street
Halifax, Nova Scotia B3J 3S8
judith.ferguson@nspower.ca

Adam Kardash
Partner & Co-Chair
Privacy and Data Management
Osler, Hoskin & Harcourt LLP
Box 50, 1 First Canadian Place
Toronto, ON M5X 1B8
akardash@osler.com

Dear Ms. Ferguson and Mr. Kardash:

M12273 - Board Inquiry into NS Power Inc.'s Cybersecurity Incident - Monthly Update #1 and Confidentiality

This letter relates to NS Power's filing of its first Monthly Update filed on August 20, 2025, and the letter of the same date of NS Power's external counsel responding to confidentiality issues about NS Power's filings in this inquiry.

The Board panel considering this matter is Stephen T. McGrath, K.C., Chair; Roland A. Deveau, K.C., Vice Chair; and Richard J. Melanson, LL.B, Member.

Monthly Update #1

On July 14, 2025, the Board directed NS Power to file monthly progress reports about its response to the recent cybersecurity incident that impacted NS Power (Incident) and its progress in preparing the requested report about the Incident (Incident Report), with the initial progress report to be filed no later than August 1, 2025. In a letter dated August 1, 2025, NS Power asked that the filing date of its first update be extended until a further date set by the Board pending clarification of the process that will apply in NS Power's filings about confidentiality. The Board granted the extension request, but directed NS Power to file any request it intends to make around confidentiality or other process issues no later than August 15, 2025.

Monthly Update #1 was filed on August 20, 2025. The items addressed included:

- On April 25, 2025, NS Power identified a cybersecurity incident resulting from unauthorized access to its information technology (IT) infrastructure. The Company immediately started containment, remediation and investigation efforts, engaging third-party cybersecurity experts and notifying the appropriate law enforcement authorities;
- The Company has started the preparation of its Incident Report on the matters outlined by the Board;
- The Incident has not caused any disruption to NS Power's generation, transmission and distribution facilities, and has not impacted the Company's "ability to safely or reliably serve customers";
- However, the Incident has impacted some business systems housed in the Company's data center, including those supporting enterprise resource planning, customer billing, energy trading, and underlying technology infrastructure such as servers, networks, and data storage;
- NS Power has established a Recovery Program Office to oversee and support the restoration of its business systems and processes. The Office has "centralized leadership, ensuring alignment across workstreams, and facilitating decision-making". NS Power said this "coordinated approach allows us to efficiently manage resources, monitor risks, and maintain clear communication with end users, all while prioritizing the safe and secure return to full operational capability";
- The Company is cooperating with the Office of the Privacy Commissioner of Canada, which has started an investigation into the Incident.

The update's content was underwhelming. It repeated information that generally was already provided in prior correspondence, and in the public domain. The Board would have expected more information about the Recovery Program Office, who is involved in that office, and the timeline for its work to be completed.

As the Company is aware, the Board has received many letters of comment and emails from NS Power's customers expressing their concerns, frustrations and complaints about the compromise and misuse of their personal information, the risks relating to the release of their personal information, and difficulties encountered in communications with the credit monitoring service engaged by NS Power. Board staff issued Information Requests (IRs) to NS Power on July 24, 2025, about frequently raised concerns and questions from customers. On August 14, 2025, due to ongoing work relating to the cybersecurity matter, NS Power requested, and was granted, extra time to provide its IR responses from August 15 to September 5, 2025. Since the Board intended that NS Power's responses be available to customers who may be seeking answers to their questions and concerns, the Board noted that it would be helpful if there was anything that NS Power could do to put more of a priority on providing these responses earlier than September 5, 2025, if that was possible. The IR responses were filed on September 5, 2025.

In terms of the Monthly Update itself, the Board would have expected more detail about the impact of the cybersecurity incident on its business systems and how it is affecting customers, interested parties and any ongoing regulatory matters before the Board. The Monthly Update did not address such matters. Instead, the Board, and parties

involved in matters before the Board, have learned about the impact of the cybersecurity incident in a haphazard manner through filings on various other matters, including:

- M12351 – The Company's Dispatch Study Action Plan Quarterly Update dated June 30, 2025, advised that the incident impacted the project's expected progress and implementation date and that the ECC Optimization Tools project schedule recovery plan and new implementation dates remain unknown;
- NS Power wrote to the Board on July 18, 2025, requesting an indefinite extension to file its 2024/25 Time-Varying Pricing (TVP) (Year Four) report and annual Evaluation, Measurement and Verification (EM&V) report due July 31, 2025. NS Power indicated the systems required to access the Advanced Metering Infrastructure (AMI) data remain currently unavailable because of the cybersecurity incident and the Company was unable to complete its work. The Company said efforts to restore the affected portions of its IT systems are ongoing, but it did not yet have a timeframe for the availability of the systems required to finalize the Year Four Evaluation Report;
- On a related but separate matter, the Company added in its July 18, 2025, letter that it is also assessing the implications of the cybersecurity incident for the upcoming TVP Season scheduled to begin November 1, 2025, and anticipates filing a proposed approach for the 2025/26 TVP Tariffs, for the Board's consideration, in the coming weeks. Typically, to ensure revised TVP rates are in effect by November 1st each year, NS Power would apply for the revised rates by July 31st (see Matter M11822). The Board also notes this application involves significant stakeholder consultation, which is hampered by the unavailability of data;
- M11626 – In its report on the Hosting Capacity Analysis Stakeholder Workshop related to the Commercial Net Metering Program, NS Power stated that the cybersecurity incident impacted some of its business applications such that the hosting capacity map and table "remain temporarily unable to be updated. This is expected to affect the timeline for planned 2026 enhancements". NS Power did not have an estimated timeframe for restoring the hosting capacity map or implementing enhancements and said it would provide updates through its Commercial Net Metering Program annual reports. The next report is due in 2026. The Board observes that the hosting capacity map is relied upon by many parties trying to connect to NS Power's grid;
- Stephen MacDonald, President and Chief Executive Officer of EfficiencyOne (E1), updated the Board on August 21, 2025, on E1's Residential Behaviour Program. He advised that the cybersecurity incident affected NS Power's capacity to transfer customer consumption AMI data to E1 and its program delivery partner. Without NS Power's AMI usage data, customer reports and insights cannot be generated and E1 is unable to measure changes in customer usage between treatment and control group customers. Accordingly, E1 was required to suspend the Residential Behaviour program and there is no confirmed timeline from NS Power about when data feeds will resume. Mr. MacDonald stated this is anticipated to materially impact E1's ability to achieve program component targets in 2025 and it is in discussions with its program delivery partner to ensure all discretionary costs are suspended during this interruption;

- M12330 - In its Q2 2025 Quarterly Report, NSPML advised that due to the cybersecurity incident, the detailed allocation between the Maritime Link Project and sustaining capital costs is unavailable at this time. It added that an update will be provided once the systems are restored. Due to the cybersecurity incident, NSPML has also requested extensions related to some of its filings to the Board. To the extent that NSPML relies on NS Power's IT systems to prepare its filings, it would be helpful for NS Power to advise on the restoration of these services;
- M12457 – A NS Power customer under the Commercial General Demand Rate (11) has complained to the Board that NS Power was unable to remotely read the customer's smart meter, it appears due to the cybersecurity incident. This required the meter to be read manually but could not be reset at the end of the billing cycle, causing the customer to be billed inflated charges on the demand charges. This is among many letters and emails, including many residential customers, about billing issues arising from the cybersecurity incident;
- M11884 – In a report dated August 29, 2025, following a directive by the Board, NS Power confirmed that replacing its existing customer information system (CIS) has been "temporarily paused" by the recent cybersecurity breach. Replacing the existing CIS system is expected to include enhancements to enable new tariff designs such as time-of-use, critical peak pricing, real-time pricing, and time varying pricing; and accommodate new programs such as Green Choice. NS Power stated that Capital Work Order C0021835 - IT - CIS Replacement was listed in the 2025 ACE Plan (M12012) as a project for subsequent submittal and that approximately $1.6 million had been spent on the project, with a projected spend of $2.2 million in 2025, and a project total of $77.9 million. Appendix B in the 2025 ACE Plan filing also indicated this project has a risk rating of 25. The Board understands it is the highest risk rating under NS Power's Asset Management Criticality & Condition Risk Alignment Matrix, which indicates this is a high-risk project requiring mitigation. NS Power said its investigation into the cybersecurity incident "could impact the direction and timeline" of the project.

The above impacts are known to the various participants in each of the matters, but there appears to be no coordinated communication of these impacts to interested parties (and to the Board), and they are only advised on an ad hoc basis as these matters arise. These impacts from the cybersecurity incident affect many customers and how interested parties interact with the Company. The Board would have expected these various impacts to be collected in a combined reporting and included in NS Power's Monthly Update. This reporting should have included the steps taken to address these impacts and the timeline to restore these issues. The Board so directs.

The next Monthly Update is due October 1, 2025, and continuing the first day of each month thereafter, without any delays.

As noted above, NS Power's IR responses were filed on September 5, 2025, and are being reviewed by the Board. Those matters will be addressed under separate correspondence.

Confidentiality

NS Power has raised confidentiality issues relating to the filings in this matter. In a letter dated August 8, 2025, NS Power requested that the Board issue a procedural order regarding the process for the Board's inquiry into the incident and that the Board find that NS Power's confidential submissions in support of the "procedural order" application be held in confidence by the Board and made available for review only by (i) the Board panel members involved in the Inquiry; (ii) the Clerk of the Board; and (iii) Board counsel.

In its response dated August 12, 2025, the Board stated:

> …the Board appreciates it will not be possible to publicly disclose some information in this proceeding for security reasons and to mitigate impacts relating to personal and confidential information that was stolen. However, the Board emphasized [in a letter dated July 14, 2025] that it was important that this proceeding be conducted as publicly and transparently as possible.
>
> The "Board Confidential" letter that you sent on August 8, 2025, does not sufficiently recognize that the Board's regulatory processes are based on the "open courts" principle and does not reflect the Board's requirement that this process be conducted as publicly and transparently as possible. In particular, it is not clear to the Board why much, if any, of your nine paragraph "Board Confidential" letter could not have been publicly disclosed, let alone disclosed to intervenors and provided under a confidentiality undertaking under the Board's normal processes. Much of the information appears to have already been publicly disclosed, is broad or general in nature, or simply states a position rather than disclose anything that appears particularly sensitive. The Board therefore requires that detailed and specific submissions be provided for each and every paragraph of the "Board Confidential" letter justifying why what is stated in each paragraph must be maintained confidentially.
>
> The additional information requested in this letter must be filed by Wednesday, August 20, 2025. Except where necessary to maintain confidentiality, this additional information must be publicly filed. If confidentiality is claimed, each instance where it is claimed must be fully justified so the basis for each claim can be fully understood and separately considered. The justification must address not only the basis for the claim, but also why the information cannot be disclosed to intervenors under a confidentiality undertaking or with other protections.
>
> [Board Letter, August 12, 2025, p. 3]

NS Power replied on August 20, 2025. First, referring to the investigations of various "privacy regulatory authorities" and their extensive experience investigating cybersecurity incidents, it submitted that their investigative procedures were helpful and informative to the Board as it determines the process it will adopt for this matter. It submitted information received in such privacy investigations was generally carried out confidentially and that disclosure was only provided in limited circumstances. It provided excerpts of statutory provisions under Canadian and European privacy legislation about such entities. Second, on the issue of confidentiality, it acknowledged it was not its intention to prevent the Board from disclosing "Board Confidential" information to the Board's advisors, but it assumed that any external

advisors will execute a confidentiality undertaking prior to their receipt of such confidential data. It added:

> 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.
>
> [Osler Letter, August 20, 2025, p. 2]

In its response, NS Power also provided confidential reasons (in its Appendix B) why NS Power's confidential submission of August 8, 2025, should be held in confidence by the Board. However, NS Power consented to the Board disclosing Appendix B and the Confidential Submission to the Formal Intervenors in this matter, under the Board's normal process for confidentiality undertakings.

As the Board has previously stated in prior correspondence in this matter, it understands that NS Power is concerned about the sensitivity of the information to be provided and intends to seek Board approval to provide information confidentially during this inquiry. However, the Board is not a privacy regulatory authority as described by NS Power's counsel. It is an economic regulator that has general oversight over NS Power and other public utilities in the province, including its function as a regulator that considers whether the utilities are providing safe and reliable service to its customers. It regulates in the public interest. The "open courts" principle applies to its processes.

The Board notes that it does not usually, and will not in the present matter, require its external advisors (including but not limited to MNP Digital) to execute a confidentiality undertaking prior to their receipt of information from NS Power. However, the Board's engagement of advisors and consultants generally includes obligations to maintain and safeguard the confidentiality of information received in the performance of their engagement.

That said, NS Power's acknowledgement that the confidential material can be reviewed by intervenors who have formal standing in this matter and who have executed a confidentiality undertaking is consistent with the process usually applied by the Board in dealing with confidential filings. The Board directs NS Power to file a draft confidentiality undertaking for its approval. The Board has reviewed confidential Appendix B to its August 20, 2025, letter, outlining the reasons why NS Power's confidential submission of August 8, 2025, should be held in confidence. The Board is satisfied that both Appendix B and NS Power's confidential submission of August 8, 2025, should be treated as confidential, subject to the Board's usual direction that this is subject to the intervenors raising objections to some of the redactions.

Finally, as noted above, the Board understands that NS Power is concerned about the sensitivity of the information to be provided and that it will seek Board approval to provide information confidentially during this inquiry. If at any time the Board or an intervenor raises a concern about NS Power's reasons for confidentiality, the Company will be afforded the opportunity to further explain why it is necessary to hold the designated information in confidence, including through a process that is appropriate in the circumstances, with the assistance of cybersecurity experts engaged by the parties.

Yours truly,

Crystal Henwood

Crystal Henwood
Clerk of the Board

c. William Mahody, K.C., Board Counsel
Parties M12273