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

July 14, 2025

judith.ferguson@nspower.ca

Judith Ferguson
Executive Vice President, Regulatory, Legal and Business Planning
Nova Scotia Power Incorporated
P.O. Box 910, 1223 Lower Water Street
Halifax, Nova Scotia B3J 3S8

Dear Ms. Ferguson:

M12273 – Board Inquiry into Nova Scotia Power's Cybersecurity Incident

This is further to my letter of May 14, 2025, advising that the Board has opened a proceeding to inquire into Nova Scotia Power's cybersecurity incident. The 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.

The Board has engaged MNP Digital to assist with the investigation and NS Power has already provided a high-level briefing about the incident for MNP, Board staff and Board Counsel.

The Board understands that NS Power's response to this incident and its own investigations are ongoing.

For the purposes of the Board's proceeding, the Board will require a report from NS Power about the incident. While not intended to limit the content of this incident report, it should include the following:

Incident Description

- A detailed account of how NS Power discovered the breach.
- A description of the attack vector.
- A timeline of events from detection to resolution.

Affected Systems and Data

- An identification of compromised systems and data.
- Specific details about the type and amount of personal information exposed.

Indicators of Compromise

- A description of evidence and artifacts indicating the presence of the breach, such as unusual network traffic or suspicious files.
- Whether NS Power was aware of activity prior to the breach that could have caused it to be alerted about a potential breach.

Root Cause Analysis

- A description of how the breach occurred.
- An identification of vulnerabilities or security gaps that were exploited.

Impact Analysis

- Assessment of the breach's impact on NS Power, including financial, operational (including operation of the grid and its communication with customers such as AMI meters, outage map, web-based customer service interfaces, and service connection requests), and reputational damage.
- Evaluation of the potential harm to NS Power's existing and former customers, and employees.

Response and Recovery Actions:

- Steps taken by NS Power to contain and mitigate the breach.
- Actions taken by NS Power to eradicate the threat and restore affected systems.
- NS Power's communication with stakeholders, including customers, employees, NERC, NPCC, E-ISAC, Canadian Centre for Cyber Security, and regulatory bodies.
- An analysis of what went well with NS Power's response to the incident and what NS Power can improve.

Collection and Retention of Personal Information:

- A review of NS Power's policies and practices for the collecting, use and retention of personal information to identify any policy or compliance gaps that affected the type and amount of personal information exposed.

Recommendations:

- Recommendations for, among other things:
    - enhancing NS Power's security measures and preventing future breaches.
    - additional security audits, policy updates, and employee training.
    - implementing new strategies and proactive measures to strengthen NS Power's cybersecurity defenses.
    - improving communications and responsiveness to the concerns and needs of NS Power's impacted customers.
    - strengthening and addressing gaps in the collection and retention of personal information.

While the Board appreciates that it will not be possible to publicly disclose certain information for security reasons and to mitigate impacts relating to personal and confidential information that was stolen, it is important that the Board's inquiry be conducted publicly and as transparently as possible. Special considerations and procedures may be required when sensitive information is involved. Issues relating to this may be raised with Board Counsel at any time.

Once NS Power's incident report is filed with the Board, the Board will establish a public process to review the report and NS Power's planning for and response to the event that occurred. The Board believes NS Power should be able to file this incident report by the end

of this year, but if NS Power does not believe this date is achievable, it may propose another.

Pending the filing of the incident report with the Board, NS Power is directed to file monthly progress reports about its response to the event and its progress in preparing the requested incident report. The initial progress report should be filed no later than August 1, 2025.

In addition to the foregoing, MNP will continue to independently assess this incident on behalf of Board Counsel and staff, to facilitate the Board's review of the incident report when it is filed. The Board directs NS Power to facilitate MNP's review and assessment of this matter, including responding to requests for information and interviews.

Finally, the Board has received numerous letters and emails from NS Power's customers expressing 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. These have been included as Letters of Comment in the open proceeding relating to this matter. Board staff have prepared information requests for NS Power, touching on frequently raised concerns and questions from customers. The Board staff information requests will be issued shortly, and responses will be due three weeks after the date they are issued.

Yours very truly,

Lisa Wallace

for Crystal Henwood
Clerk of the Board

c. William L. Mahody, K.C., Board Counsel
MNP Digital
Interested Parties