M12600

NOVA SCOTIA ENERGY BOARD

IN THE MATTER OF: ***The Public Utilities Act***

– and –

IN THE MATTER OF: **AN INQUIRY** about the impact of the cyber incident on **NOVA SCOTIA POWER INCORPORATED's** collection and retention of customer information, customer service and communications, billing processes and regulatory matters

INFORMATION REQUESTS

To: **Blake Williams**
Senior Director, Regulatory Affairs
Nova Scotia Power Inc.
1223 Lower Water Street
Halifax, NS B3J 2A8
Email: blake.williams@nspower.ca

From: The Consumer Advocate

Responses Due: **May 6, 2026**

Copies: 1 electronic copy (PDF searchable)

Contact Person: **David J. Roberts**
Consumer Advocate
Pink Larkin
1463 South Park Street
Halifax, NS B3J 3S9
Tel: (902) 423-7777
Email: droberts@pinklarkin.com

Request IR-1: Cyber Security Program Effectiveness

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 18, ll 1-4

Quote:
NS Power maintains a cybersecurity training and awareness program and conducts mandatory quarterly cyber training and monthly phishing simulation testing exercises with all employees to educate employees about NS Power's information security policies and common risks, and to help them understand their information security responsibilities.

Question

a. For the twelve-month period ending March 2025, please provide the results of the quarterly cyber training and monthly phishing simulation testing.

b. Please describe NSPI's training standards for cybersecurity. How frequently are employees required to be tested?

c. What percentage of NSPI's employees had completed training consistent with NSPI's standards at the time of the Incident and as of the most recent date available.

d. What are NSPI's targets and/or metrics for cybersecurity readiness; for example, what is the target for phishing success?

e. Please provide a summary of the number and types of cyber incidents NSPI recorded in the last 5 years? What improvements have been made to systems and practices as a result of these events.

Request IR-2: Customer Data Retention

Reference: NSPI Customer Privacy Policy

Quote:
The length of time we keep your information varies depending on the product or service in question and the nature of the information. We have retention standards that allow us to meet customer service, legal and regulatory needs. As a result, it may be necessary for us to keep some of your information on record even after the end of your relationship with us. When the information is no longer required, it is destroyed or anonymized.

Question

a. Please provide the retention standards referenced in the above quote.

b. Please confirm that these standards are compliant with the Personal Information Protection and Electronic Documents Act (PIPEDA).

Request IR-3: Customer Data Retention

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 40, ll. 10-24

Quote:
With respect to the collection and retention of customer social insurance numbers, as noted in Peter Gregg's opening statement to the Standing Committee on Natural Resources and Economic Development on November 25, 2025, appended to NS Power's December 1, 2025 Incident monthly update report, "Except for tax reporting purposes, we no longer collect social insurance numbers and are on track to complete their removal from our systems by March 31st."

Prior to 2018, it was NS Power's practice to collect social insurance numbers (SINs) from customers as part of authentication and identification of a customer during the account opening process. In 2018, NS Power changed that practice and no longer collected SINs (except in limited circumstances detailed below).

Subsequently in 2019, Customer Service Representatives were instructed to remove SINs for the Customer Information System (CIS) whenever a SIN was encountered within CIS. In May of 2024, NS Power developed and commenced a process to purge customer SINs from the CIS environment.

Question

a. Please confirm that NSPI has purged all customer SINs from NSPI systems.

b. Based on the above quote, NSPI was aware in 2018 the Company had collected customer SIN without a valid business reason as required by PIPEDA. Please explain why, as of the date of the incident, NSPI had not expunged this data from its systems.

c. Please provide the number of closed accounts for which NSPI still had customer SIN information at the time of the incident in the following categories:

i. Account closed less then one year before the Incident

ii. Account closed between one and two years before the Incident

iii. Account closed between two and five years before the Incident

iv. Account closed between 5 and ten years before the Incident

v. Account closed more than 10 years before the Incident

Request IR-4: Data Retention Policy Compliance with Legislation

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 40, ll 3-5

Quote:
At the time of the Incident, NS Power had formally documented its approach to privacy compliance through an established and robust suite of written privacy policies, procedures, and related documentation, including which govern its collection, use and retention of personal information.

Question

a. Please explain the process NSPI uses to determine what personal information can legally be collected from customers?

b. Please provide the results of the last available audit or review conducted by an independent third party on NSPI data collection and retention policies; if no such audit or review exists, please explain how NSPI assesses the legality of data collection practices and the frequency for this assessment.

c. Please explain, with reference to appropriate authorities, on what legal basis NSPI retains customer data after the closure of accounts.

d. What personal information does NSPI currently collect from customers and for what reason?

e. Please provide the number of closed accounts for which NSPI had retained customer information at the time of the Incident.

f. Were NSPI's customer information records in compliance with all of NSPI's relevant privacy and security policies and procedures at the time of the incident? If not, please provide a detailed discussion of the areas that were not in compliance and the steps taken since the Incident to bring the customer information records into compliance and ensure compliance going forward.

g. What personal information currently collected from customers by NSPI is retained?

    i) For how long and for what reason?

Request IR-5: Customer Account Collections

Reference: Exhibit 100853 - NS Power's Monthly Update #2, page 7

Quote:
In acknowledging that customers' billing experience was impacted by the Incident, NS Power has waived all late fees and paused collections activity since the Incident.

Question

a. Please provide NSPI's customer account collection policies that were in effect as of the date of the incident.

b. Please confirm that no customer accounts have been sent to credit collection agencies since the date of the incident. If not confirmed, please provide the number of accounts that have been sent to credit collection agencies since the Incident and explain why some accounts continued to be sent for collection.

c. Has NSPI received any complaints from customers about late fee charges or referrals to collection agencies? If yes, please quantify the number of complaints and describe NSPI's actions to address these complaints.

Request IR-6: Treatment of Incident Costs

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 14, ll 18-25

Quote:
Immediately following detection of unauthorized access, NS Power activated its incident response and business continuity protocols, engaged leading third-party cybersecurity experts, and took actions to contain and isolate the affected servers and prevent further intrusion. Since the discovery of the event, NS Power has mobilized a team of internal and external specialists to support the recovery effort. The Company's immediate priorities focused on containment, eradication and remediation of the threat, and conducting a thorough analysis to understand the full scope and nature of the Incident.

Question

a. Please quantify the costs incurred to date to respond to the Incident and provide a forecast of any remaining costs NSPI anticipates incurring through December 31, 2027. Please include both internal costs and any external contracting costs.

b. Please explain how NSPI is isolating the costs associated with the incident to ensure that ratepayers will not be required to pay any of these costs now or in the future.

c. Please discuss how many staff (FTEs) were reassigned from regular duties to respond to the Incident. Please comment on the implications for operations and customer service levels as a result of any staff being reassigned.

d. How many staff (FTEs) originally reassigned from regular duties to respond to the Incident are still being reassigned?

Request IR-7: Cybersecurity Risk Management

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 17, ll 11-24

Quote:

NS Power's cybersecurity framework (which applies to its information technology program more generally) includes specific policy and control standards aligned with NIST's Core Functions as noted below:

- Identify – Establishes organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Establishes the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Establishes the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Establishes the appropriate activities to take action regarding a detected cybersecurity event.
- Recover – Establishes the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Question

a. Does NSPI carry insurance for cybersecurity events

   i. If yes, please provide copy of policy documents and claims documents, if any;

   ii. If not, please explain why not.

b. Please explain the steps by which the unauthorized third party was able to gain access to NSPI's information technology systems.

c. What was the triggering event that allowed the unauthorized third party access?

d. What measures have been put in place that will prevent unauthorized third party access to NSPI's information and technology systems if the triggering event was to be repeated?

Request IR-8 - Customer Risk Mitigation

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 38, ll 25-28, Page 39, ll 1-3

Quote:

Provided guidance to customers for steps they could take to reduce any risk of harm resulting from the incident (including steps to protect themselves from fraud or potential identity theft). This notice included an offer for two years of complimentary credit monitoring and identity monitoring

services for impacted individuals. The Company subsequently extended the offer of complimentary credit monitoring to five years on June 2 25, 2025. Customers who had already registered for credit monitoring had their offer automatically extended.

Question

a. Does NSPI view the provision of credit monitoring services as fulfilment of any future liability to customers for damages resulting from the loss of customer data from NSPI systems?

Request IR-9: Data Breach Mitigation

Reference: Exhibit N-3 - 2025 Nova Scotia Power's Cybersecurity Incident Report, Page 38, ll 25-28

Quote:
The Company adopted a best-practices approach to mitigating potential harm to customers whose personal information was impacted by the Incident. This approach was grounded in a commitment to transparency, timely communication, and a customer-centric focus. The Company's objective throughout has been to provide affected individuals with meaningful support, reduce the risk of harm, and maintain trust through accountability.

Question

a. How did NSPI determine this approach was "best-practice"?

b. Please provide a list of mitigation measures that were considered but not implemented and explain why.

c. Did NSPI consider financial relief, credits or bill smoothing options for the affected customers?

   i. If not, why not?

Request IR-10 - Customer Impacts

Question

a. For each month following the Incident up to and including the most recent month of actuals available, please provide:

   i. The total number and percentage of customer bills that were estimated.

   ii. The number of customer complaints received related to estimated bills.

iii. Any customer service metrics tracked by NSPI such as time on hold, dropped calls or other similar metrics.

Where data for a particular month are not available either due to the impact of the Incident or other reasons, please provide an explanation.

b. Please provide any policies or procedures NSPI had in place for responding to customer complaints with respect to estimated or inaccurate bills.

c. What method was employed to estimate bills for customers?

e. What, if any, changes were made to the methods used to estimate customer bills since the discover of the cyber incident. If no changes were made, does NSPI intend to undertake a review to inform future potential changes? Why or why not?

f. For customers whose estimated bills resulted in material overpayments, does NSPI credit customers for interest on credit balances? If not, why not?

Request IR-11: Customer Notification

Reference: Response to NSEB IR-1 in Proceeding M12273

Quote:
"NS Power developed and implemented a consistent multi-channel approach throughout the response efforts for all public communications. For each update, the transparency effort involved postings on the Company website and social media channels, notice to all local media, and communications directly to key account/business customers, government and other stakeholders in addition to employees."

Question

a. Please describe any specific methods or communication channels NSPI used to try to reach former customers, particularly customers whose contact information in NSPI's records may no longer be up to date and/or who may no longer live in Nova Scotia to alert them about the Incident.

b. Did NSPI adapt or modify its communications plan based on customer feedback at any point? If so, please describe changes made based on customer feedback.

c. Has NSPI undertaken a review the effectiveness of its communication methods? If so, please provide a summary of any key findings. If not, does NSPI plan to complete such a review? Why or why not?