M12600

NOVA SCOTIA ENERGY BOARD

IN THE MATTER OF: *The Public Utilities Act,* R.S.N.S. 1989, c.380, as amended

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 (NON-CONFIDENTIAL)

To: **Blake Williams**
Vice President, Legal and Regulatory
Nova Scotia Power Incorporated
P.O. Box 910
1223 Lower Water Street
Halifax, NS B3J 3S8
By email: blake.williams@nspower.ca

From: Small Business Advocate

Responses Due: May 6, 2026

Copies: 1 electronic copy (PDF searchable)

Contact Person: **Melissa P. MacAdam**
Blackburn Law Inc.
Small Business Advocate
Phone (902) 835-8544
mmacadam@blackburnlaw.ca

Issued at Bedford, Nova Scotia on this 22nd day of April, 2026

Request IR-1:
Please refer to M12600, Exhibit N-3, Nova Scotia Power Incident Report - Redacted, dated December 22, 2025 (the "Report"), Page 7, Lines 23-24:

> The Incident was discovered on April 25, 2025, when NS Power employees reported certain applications on the Company's systems were not functional…

a) Was that the first time those applications were non-functional?
b) Has Nova Scotia Power Inc. (NS Power) confirmed that no other employee had noticed issues with those applications before April 25, 2025 and did not report it?
c) Did one or multiple people report the issue with the applications on April 25, 2025?
d) How many applications were first noticed to have an issue?

Request IR-2:
Please refer to the Report, Page 8, Lines 1-3:

> Immediately following detection of the Incident, NS Power activated its established incident response and business continuity protocols, engaging Osler, and through Osler, Mandiant's cybersecurity and incident response team.

a) What are the "established incident response and business continuity protocols" (the "Protocols") and who within NS Power is responsible for them?
b) How were they developed? Are they written down?
c) How often are the Protocols updated?
d) In preparing the Protocols, was there any research done on previous incidents experienced by NS Power or other similar entities (for example NERC, the Electricity Information Sharing and Analysis Center, and the Northeast Power Coordinating Council)?
e) Was there any research conducted on other similar entities' protocols, their experiences or any learnings they may have? If so, please provide details about the other entities and how the information gathered was incorporated into the Protocols.
f) What was Osler's role in response to the Incident?

Request IR-3:
Please refer to the Report, Page 8, Line 19-22:

> NS Power notified law enforcement of the Incident. More specifically, NS Power notified the Canadian Centre for Cybersecurity (CCCS), the Royal Canadian Mounted Police (RCMP), and the Canadian Security Intelligence Service (CSIS) on April 27, 2025 and provided them with information about the Incident.

a) Why was there a gap from April 25, 2025, when you first became aware of the issue, and the notification of law enforcement on April 27, 2026?
b) When did you notify the Federal Bureau of Investigation (FBI)?
c) Was there a discussion of when to tell the different law enforcement entities? Did NS Power receive advice on when the notification should take place?
d) Was there anything in the Protocols about who should be notified and when the notifications should be done?

Request IR-4:
Please refer to the Report Page 8, Lines 27 - 28:

> NS Power also reported the Incident to the Office of the Privacy Commissioner of Canada (OPC) on May 1, 2025, with an update on May 14, 2025.

a) Why was there a gap from April 25, 2025, when you first became aware of the issue, and the notification of OPC on May 1, 2026?
b) Did any of the law enforcement agencies you notified on April 27, 2025 mention or recommend notifying OPC?
c) Was there a discussion of when to tell OPC? Did NS Power receive advice on when the notification should take place?

Request IR-5:
Please refer to the Report, Page 26, Lines 22-24:

> NS Power also notified NERC, the Electricity Information Sharing and Analysis Center (E-ISAC), and the Northeast Power Coordinating Council, and provided them with information about the Incident.

a) When were the above noted notifications made?
b) Was there a discussion of when to tell these entities? Did NS Power receive advice on when the notification should take place?
c) If the notification took place after April 25, 2025, what was the reason for the delay?
d) Did any of these entities provide advice or instructions to NS Power as to how to address or respond to the Incident? If so, what was that advice/instructions?

Request IR-6:
Please refer to the Report, Page 17, Lines 3-6:

> At the time of the Incident, NS Power had implemented a common set of cybersecurity standards and policies that are informed, in part, by the National Institute of Standards and

Technology's (NIST) Cybersecurity Framework, and the Company regularly reviews and makes continuous improvements to its cybersecurity programs to ensure it is in line with the latest guidance.

a) Are the 'cybersecurity standards and policies' (the "Policies") same or different from the Protocols referred to on Page 8 of the Report? If different, please explain the differences between them and how they apply to this Incident.
b) The Policies referenced in the quote above are described as having been "informed, in part" by the NIST Cybersecurity Framework. Was that the only source that informed the development of the Policies?
c) What is meant by "regulatory reviews" - is there a specific time frame in which they must be reviewed? Is the timing of the reviews based on incidents that happen elsewhere? Where does the 'latest guidance' come from?
d) Do you get updates and/or guidance on issues from other organizations, like NERC/E-ISAC/the Northeast Power Coordinating Council etc?

Request IR-7:
Please refer to the Report, Page 17, Lines 19-20:

Detect – Establishes the appropriate activities to identify the occurrence of a cybersecurity event.

a) Did the 'Detect' part of the Cybersecurity Framework operate as expected?
b) If yes, why was there a delay between when the breach happened and when you became aware of it?
c) If no, have you confirmed why it did not operate as expected? Please provide details.

Request IR-8:
Please refer to the Report, Page 17, Lines 26-20:

In relation to NS Power's operational program, NS Power's core energy operations are designed to comply with other industry-specific rules and standards relating to cybersecurity and IT including, but not limited to, those mandated by the North American Electric Reliability Corporation (NERC). NERC conducts extensive periodic audits (including security) of the Company's Energy Operations to ensure effective compliance.

a) When was NSP last audited by NERC with respect to cybersecurity or IT?
b) Does NERC produce a report of its audits? If so, please provide the most recent one that addresses NS Power's cybersecurity and IT operations.

Request IR-9:
Please refer to the Report, Page 18, Lines 1-4:

> 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.

a) What does the 'mandatory quarterly cyber training' include?
b) Is there a test or evaluation completed as part of the training? If so, how is it marked and what is considered a pass? What happens if someone does not pass?
c) Do you document 100% participation in the mandatory quarterly cyber training and the pass/fail information, if applicable? Please provide any information about the percentage of participation and pass/fail ratings for the past 3 years.
d) With respect to the monthly phishing simulation testing exercises, are these sent to all employees every month? If not, how long would it be before every employee had been contacted with respect to the phishing simulation testing exercises (ie how many months to confirm that 100% of employees had been contacted)
e) Do you track the success/failure of phishing simulation testing exercises? Is it pass/fail or based on a scale? What happens if an employee fails the testing exercise? What are the rates (either pass/fail or scale based) for the past 3 years?
f) Has NS Power made any changes to its cybersecurity training and awareness program, quarterly cyber training and monthly phishing simulation testing exercises, information security policies, the Policies or Protocols, since the incident? Please provide details and when the changes were implemented or, if not yet implemented, when they are expected to be implemented.

Request IR-10:
Please refer to the Report, Page 18, Lines 19-29:

> NS Power implemented a previously developed and tested consistent multi-channel approach throughout the response efforts for all public communications. For each update, the transparency effort involved postings on a dedicated cyber update landing page on the Company's 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.
>
> To ensure customers were kept informed, the Company also employed a multi-platform paid media strategy that includes online, as well as TV, print and radio to reach a wide variety of customer demographics. In addition, NS Power activated a paid search strategy throughout the Incident to
> ensure that the NS Power website and information appeared as the top search result when customers used search engines (i.e. Google) to find information about the Incident. throughout the response efforts for all public communications…

a) When was the multi-channel approach first implemented for this Incident?
b) When was the paid media strategy implemented? Who bears the cost for the paid media strategy?

Request IR-11:
Please refer to the Report, Page 19, Lines 8-9:

> As noted above, the Company became aware of the Incident on Friday, April 25, 2025. The next business day, on Monday, April 28, 2025, NS Power informed customers that it was actively responding to a cybersecurity incident and encouraged customers to report any suspicious emails or phone calls.

a) How did NS Power first notify customers?
b) Was there a discussion of when to notify customers? Did NS Power receive advice on when the notification should take place?

Request IR-12:
Please refer to the Report, Page 25, Lines 22-23:

> As discussed elsewhere in this report, part of the internal process related to this incident will include a review of lessons learned, including a review of communications with customers.

a) Will the "lessons learned" report be provided the Board and stakeholders?
b) If yes, when is it expected to be completed?
c) If no, why not?

Request IR-13:
Please refer to the Report, Page 37, Lines 15-16:

> …In connection with these efforts, NS Power has recently completed an extensive two-year update to its cybersecurity practices to comply with current policies and anticipated changes in standards communicated by NIST.

a) When was the two-year update completed?

Request IR-14:
Refer to M12600, Exhibit N-1, Nova Scotia Energy Board (NESB) IR 4(a):

> As noted above, NS Power extended the offer of credit monitoring by three additional years beyond the two-year industry standard, providing additional protection for delayed impacts

of the breach and made the credit monitoring available to all current and former customers…

a) Is the 'industry standard' referred to in the quote about referingto the electricity industry, with respect to security breaches, or to another industry?
b) How did NS Power determine the 'industry standard'?
c) At this time, is NS Power aware of any identity breaches/damages suffered by a customer as a result of this Incident?

Request IR-15:
Refer to M12600, Exhibit N-1, NESB IR 6(a):

The Company's investigations remain ongoing. At this time, it is not possible to determine precisely what specific personal customer information, if any, was affected by this incident…

a) The quote about refers to "at this time" – has that changed or is it expected to change at any point in the future? If yes, when?

Request IR-16:
Please refer to the Report, Page 40, Lines 21-24:

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.

a) What is meant by "developed and commenced" a process to purge SINs? What took place between 2019, when the instruction to remove SINs was made and May of 2024 with respect to SINs? How was the process developed and commenced in 2024 different than the instructions provided in 2019?
b) Between 2019 and May 2024, does NS Power know either how many SINs were removed (or percent reduction)? Please provide as much detail as possible.
c) Between May 2024 and April 2025, does NS Power know either how many SINs were removed (or percent reduction)? Please provide as much detail as possible.

Request IR-17:
Refer to M12600, Exhibit N-1, NSEB IR 12, Page 2-3, Lines 8-9:

…Also, the Company has not applied late charges, or penalties on any outstanding balances since the incident. NS Power will communicate directly with customers before reintroducing late fees on outstanding amounts.

a) Does NS Power know when it expects to reinstate late fees?
b) Is there any financial impact on NS Power for waiving late fees? If so, what is the current estimate of that impact and who bears it?

Request IR-18:
Refer to Compliance Letter to the Office of the Privacy Commissioner of Canada ("OPC") dated March 18, 2026 (https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/2026-ns-power-ca/) (the "OPC Compliance Letter"), Breach Timeline:

- On or around April 8, 2025, the threat actor began to move laterally across systems in the Nova Scotia Power network environment, using accounts with domain administrator privileges. Between April 8 and April 22, 2025, the threat actor deployed and leveraged additional malware to perform internal reconnaissance and credential harvesting activities.

a) What protections were in place to prevent that privilege elevation, ie intended to prevent the threat actor from obtaining domain administrator privileges?
b) Was there any sort of detection mechanism in place that could have noticed the threat actors movements through the system?
c) Have you determined why the background actions were not identified between April 8-25, 2025? If yes, have you taken steps to prevent it from happening again, without notice?

Request IR-19:
Refer to Compliance Letter to the Office of the Privacy Commissioner of Canada ("OPC") dated March 18, 2026 (https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/2026-ns-power-ca/) (the "OPC Compliance Letter"), Breach Timeline:

- On April 25, 2025, the threat actor used credentials acquired during its previous credential harvesting activities to destroy backups and deploy ransomware.

a) Other than the backups that were destroyed by the threat actor, were there any other backups maintained by NS Power, such as offsite or on an immutable storage? If not, why not?

Request IR-20:
Refer to Compliance Letter to the Office of the Privacy Commissioner of Canada ("OPC") dated March 18, 2026 (https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/2026-ns-power-ca/) (the "OPC Compliance Letter"), Breach Timeline:

- Nova Scotia Power received communications from the threat actor that included a hyperlink to an unlisted page accessible through the Tor network on the dark web. The threat actor provided proof that it had obtained sensitive customer information, but no

evidence has yet emerged that this sensitive data has been made public or sold. After its assessment of applicable sanctions laws and alignment with law enforcement guidance, Nova Scotia Power did not pay a ransom to the threat actor.

a) When did NS Power first obtain proof that the threat factor had obtained sensitive customer information?