

NON-CONFIDENTIAL

Request IR-01:

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?

Response IR-01:

(a) No, NS Power had experienced outages in the past but hadn’t previously had an outage of that magnitude.

(b) Outages for some of the impacted applications had been reported prior to April 2025 but they have been confirmed to not be related to the cyber incident and it has been confirmed that they were reported prior to the date Mandiant found the first activity of the threat actor.

(c) Multiple people reported the outage.

(d) All of NS Power’s IT applications on the corporate network were impacted with the exception of our Customer Information Systems (CIS).

NON-CONFIDENTIAL

1 **Request IR-02:**

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

4
5 **Immediately following detection of the Incident, NS Power activated its established**
6 **incident response and business continuity protocols, engaging Osler, and through**
7 **Osler, Mandiant’s cybersecurity and incident response team.**

8
9 **(a) What are the “established incident response and business continuity protocols” (the**
10 **“Protocols”) and who within NS Power is responsible for them?**

11
12 **(b) How were they developed? Are they written down?**

13
14 **(c) How often are the Protocols updated?**

15
16 **(d) In preparing the Protocols, was there any research done on previous incidents**
17 **experienced by NS Power or other similar entities (for example NERC, the Electricity**
18 **Information Sharing and Analysis Center, and the Northeast Power Coordinating**
19 **Council)?**

20
21 **(e) Was there any research conducted on other similar entities’ protocols, their**
22 **experiences or any learnings they may have? If so, please provide details about the**
23 **other entities and how the information gathered was incorporated into the Protocols.**

24
25 **(f) What was Osler’s role in response to the Incident?**

26
27 **Response IR-02:**

28 **(a-e) NS Power maintains a formally documented “Cyber Incident Response Protocol”**
29 **(provided to the Board as Board Confidential Attachment 8 to the response to NSEB IR-**
30 **9), and supporting materials, which NS Power has focused on developing and enhancing**

NON-CONFIDENTIAL

1 over the past several years, based on a work effort conducted with internal stakeholders,
2 and with input from relevant subject matter experts, including in close consultation with
3 external legal counsel. The protocols are established and updated on an ongoing basis.

4 The NS Power Cyber Incident Response Protocol is designed to outline a clear process for
5 responding to a cyber incident, and is designed to reflect and integrate with relevant NS
6 Power operations and processes

7
8 NSPI's Cyber Incident Protocol is designed to serve as a flexible framework that ensures
9 the organization appropriately escalates, addresses, and responds to security incidents. By
10 design, this protocol establishes guiding principles and general procedures that enable
11 personnel to exercise informed judgment and respond effectively in real time as
12 circumstances evolve.

13
14 NS Power reviews these protocols and supporting documents on an annual basis to comply
15 with best practices, and revises the documents as necessary (i) to ensure currency with legal
16 and industry developments, and (ii) to reflect changes to roles/responsibilities, technology
17 or business processes that may impact a cyber incident response.

18
19 (f) During the course of the Incident engagement, Osler provided advice and related guidance
20 regarding the response by NS Power to the Incident, and the legal and regulatory
21 obligations and responsibilities of NS Power in connection therewith, including regarding
22 communication with stakeholders.

23
24 Specifically, in its capacity as counsel, Osler assisted with the following matters arising
25 from the Incident:

- 26
27 • **Preliminary Risk Assessment** – Attended incident response team meetings and
28 provided guidance on managing the Incident, drawing from its extensive
29 experience in incident response.

NON-CONFIDENTIAL

- 1 • **Internal Communications** – Advised and provided review support with respect to
2 communications to various internal stakeholders
3
- 4 • **Containment and Investigative Efforts** – Oversaw appropriate steps to promptly
5 contain the Incident, including collaborating with internal personnel and engaging
6 third-party service providers as necessary to assist in efforts to contain the Incident.
7
- 8 • **Risk Assessment** – Reviewed materials relating to the forensic investigation into
9 the incident, including working closely with forensic firms in its preparation of
10 various deliverables.
11
- 12 • **Data Analysis** – Based on findings from the forensic investigation, worked closely
13 with internal and external data analysis experts on the following:
14
 - 15 • Coordination of the engagement and oversight of, and liaising with, third
16 party data analysis experts;
17
 - 18 • Alignment on and review of data analysis report.
19
- 20 • **External Communications** – Drafted, reviewed and revised scripts for verbal
21 communications and written communications with key stakeholders impacted by the
22 Incident.
23
- 24 • **Notification of the Incident** – Provided advice with respect to whether there was a legal
25 obligation, or other rationale, for providing notification to impacted individuals, privacy
26 regulatory authorities, and third-party stakeholders. This included carefully considering the
27 applicable legal threshold for notification on a case-by-case basis and determining whether
28 to undertake notification to regulatory authorities and affected individuals as required
29 under applicable law.
30

NON-CONFIDENTIAL

- In particular, Osler carefully considered the relevant notification and reporting obligations, including notification to affected individuals, relevant privacy regulatory authorities, and organizations to which the Company had a contractual obligation to notify.

- Assisted with drafting individual notification letters, regulatory reporting letters, and communications to other stakeholders with respect to the Incident.

- **Credit monitoring** – Coordinated delivery of monitoring and identity protection services.

- **Law Enforcement** – Assisted with and advising on interactions with law enforcement, including calls with same.

- **Insurance Coverage** – Collaborated to regularly consider the involvement of cyber insurer and provide necessary documentation to ensure prompt and complete coverage.

NON-CONFIDENTIAL

1 **Request IR-03:**

2
3 **Please refer to the Report, Page 8, Line 19-22:**

4
5 **NS Power notified law enforcement of the Incident. More specifically,**
6 **NS Power notified the Canadian Centre for Cybersecurity (CCCS), the**
7 **Royal Canadian Mounted Police (RCMP), and the Canadian Security**
8 **Intelligence Service (CSIS) on April 27, 2025 and provided them with**
9 **information about the Incident.**
10

11 **(a) Why was there a gap from April 25, 2025, when you first became aware of the issue,**
12 **and the notification of law enforcement on April 27, 2026?**

13
14 **(b) When did you notify the Federal Bureau of Investigation (FBI)?**
15

16 **(c) Was there a discussion of when to tell the different law enforcement entities? Did NS**
17 **Power receive advice on when the notification should take place?**
18

19 **(d) Was there anything in the Protocols about who should be notified and when the**
20 **notifications should be done?**
21

22 **Response IR-03:**
23

24 **(a) As noted in Section 2.0 of the Incident Report, NS Power detected the Incident on April**
25 **25, 2025. NS Power immediately launched an investigation with the assistance of external**
26 **experts to determine the nature and scope of the Incident.**
27

28 **Based on the results of this initial investigation, and in consultation with the appropriate**
29 **internal and external experts and decisions makers (as outlined in NS Power's established**
30 **incident response protocols), determined that it would be appropriate to notify law**
31 **enforcement of the Incident.**

NON-CONFIDENTIAL

1 NS Power promptly made this notification on April 27, 2025, two days after initial
2 discovery of the Incident, at the first practically possible time in the circumstances, given
3 the timeline need to determine the nature of the Incident.

4
5 (b) NS Power notified the FBI on April 27, 2025.

6
7 (c) Please see (a) above.

8
9 (d) NS Power's established incident response protocols contemplate notification of law
10 enforcement where appropriate given the circumstances of a particular incident. The
11 decision of which parties to notify, and when this notification is appropriate is made by the
12 incident response team, in consultation with internal and external legal counsel, as was the
13 case with respect to the Incident.

NON-CONFIDENTIAL

Request IR-04:

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?

Response IR-04:

(a) See Section 4.3 of the Incident Report. Immediately following detection of the Incident, on April 25, NS Power commenced an investigation into the nature and scope of the incident, including the impacted information with the assistance of third-party experts.

On May 1, 2025, based on the results of the ongoing investigative efforts, NS Power determined that customer information had been impacted in the Incident, and promptly notified the Office of the Privacy Commissioner of Canada (OPC), in line with appropriate regulatory guidance and obligations, while it continued its data analysis efforts.

(b) No. None of the law enforcement entities mentioned or recommended notification to any regulatory authorities.

NON-CONFIDENTIAL

- 1 (c) Yes. The Company's established incident response protocols contemplate notification to
2 the OPC where appropriate given the circumstances of an incident. Fully consistent with
3 those protocols, the OPC was promptly notified about the Incident upon determining that
4 there was a potential impact to personal information held in NS Power's systems.

NON-CONFIDENTIAL

1 **Request IR-05:**

2
3 **Please refer to the Report, Page 26, Lines 22-24:**

4
5 **NS Power also notified NERC, the Electricity Information Sharing and**
6 **Analysis Center (E-ISAC), and the Northeast Power Coordinating**
7 **Council, and provided them with information about the Incident.**
8

9 **(a) When were the above noted notifications made?**

10
11 **(b) Was there a discussion of when to tell these entities? Did NS Power receive advice**
12 **on when the notification should take place?**

13
14 **(c) If the notification took place after April 25, 2025, what was the reason for the delay?**

15
16 **(d) Did any of these entities provide advice or instructions to NS Power as to how to**
17 **address or respond to the Incident? If so, what was that advice/instructions?**

18
19 **Response IR-05:**

20
21 As previously noted, in relation to the Incident, the Company continues to have no evidence the
22 threat actor accessed any operational technology or energy delivery systems, or that these systems
23 were impacted. Core operations and the electric grid continued uninterrupted – no power was lost
24 to Nova Scotians. In line with standard processes, and on a courtesy basis, notification of the
25 Incident was sent to Northeast Power Coordinating Council (“NPCC”) on April 28, 2025. NERC
26 and the Electricity Information Sharing and Analysis Center (E-ISAC) were notified on May 1,
27 2025.

28 Consistent with the Company’s established incident response protocols, the transmission system
29 operator (NSPI Energy Control Centre) was included in the immediate incident response. The
30 transmission system operator notified the Reliability Coordinator (NB Power) on April 28, 2025,

NON-CONFIDENTIAL

- 1 and arranged for the appropriate notifications to the relevant sector specific regulators. These
- 2 notifications took place as soon as practicably possible.

NON-CONFIDENTIAL

Request IR-06:

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?

Response IR-06:

(a) The protocol is the Cyber Incident Readiness Protocol that describes how to handle cyber incident whereas the Cyber Security Framework is a set of standards and policies describing the cybersecurity controls and control objectives of NS Power cybersecurity program, and is provided to the Board as Board Confidential Attachment 8 to NSEB IR-9.

NON-CONFIDENTIAL

1 (b) No, it was not the only source, the CSF was also informed by best practices from major
2 consulting firms (Deloitte and Mandiant), best practices from the Canadian Center for
3 Cyber Security (CCCS), E-ISAC, the US Cybersecurity and Infrastructure Agency (CISA)
4 and the US Department of Defense (DoD).

5
6 (c) Policies, including the Cybersecurity Framework are reviewed annually. This is the review
7 frequency recommended by NIST. Additional reviews can also be triggered if major
8 changes are recommended through NIST special publications, E-ISAC CCCS, CISA or
9 DoD recommendations.

10
11 (d) Yes, as per response C.

NON-CONFIDENTIAL

1 **Request IR-07:**

2
3 **Please refer to the Report, Page 17, Lines 19-20:**

4
5 **Detect – Establishes the appropriate activities to identify the**
6 **occurrence of a cybersecurity event.**
7

8 **(a) Did the ‘Detect’ part of the Cybersecurity Framework operate as expected?**

9
10 **(b) If yes, why was there a delay between when the breach happened and when you**
11 **became aware of it?**

12
13 **(c) If no, have you confirmed why it did not operate as expected? Please provide details.**

14
15 **Response IR-07:**

16
17 **(a) Based on the investigation, there is no evidence or reasons to think that the Detect part of**
18 **the Cybersecurity Framework was not working as expected at the time of the cyber event.**

19
20 **(b) When dealing with extremely advanced threat actors as the ones who compromised NS**
21 **Powers IT environment, it is a constant catch-up between the security detection and**
22 **prevention solutions and the innovations and novel techniques used by advanced threat**
23 **actors. It is believed by NS Power and Mandiant, the expert third-party who supported the**
24 **incident response and investigations, that at the time of the incident the technique and**
25 **malware used by the threat actor could not be detected by the security detection solution in**
26 **place at NSPI and the threat actor managed to operate in a manner that could not be detected**
27 **by our security tools.**

28
29 **(c) N/A.**

BOARD CONFIDENTIAL (Attachment Only)

1 **Request IR-08:**

2
3 **Please refer to the Report, Page 17, Lines 26-20:**

4
5 **In relation to NS Power’s operational program, NS Power’s core**
6 **energy operations are designed to comply with other industry-specific**
7 **rules and standards relating to cybersecurity and IT including, but not**
8 **limited to, those mandated by the North American Electric Reliability**
9 **Corporation (NERC). NERC conducts extensive periodic audits**
10 **(including security) of the Company’s Energy Operations to ensure**
11 **effective compliance.**
12

13 **(a) When was NSP last audited by NERC with respect to cybersecurity or IT?**

14
15 **(b) Does NERC produce a report of its audits? If so, please provide the most recent one**
16 **that addresses NS Power’s cybersecurity and IT operations.**

17
18 **Response IR-08:**
19

20 **(a) NPCC initiated an Audit for NERC Critical Infrastructure Protection (CIP) and Operations**
21 **& Planning (O&P) standards on December 6, 2024, which continued into 2025. Due to the**
22 **cyber-attack, NPCC extended the duration of the Audit with interviews completed in**
23 **September 2025 instead of May 2025. NPCC provided the final Audit report in January**
24 **2026.**

25
26 **(b) The NPCC final audit report is confidential due to the CIP information included therein.**
27 **NPCC has flagged the report as "Non-Public Version. Contains Confidential Information**
28 **Including Privileged and Critical Energy Infrastructure Information. Do Not Distribute". NS**
29 **Power is providing the report on a Board Confidential basis.**

REDACTED (CONFIDENTIAL INFORMATION REMOVED)

**Cybersecurity Accountability Board Confidential
SBA IR-8 Attachment 1 has been removed due to
confidentiality.**

NON-CONFIDENTIAL

Request IR-09:

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**

NON-CONFIDENTIAL

1 **provide details and when the changes were implemented or, if not yet implemented,**
2 **when they are expected to be implemented.**

3
4 Response IR-09:

5
6 (a) Mandatory quarterly cyber training is delivered through our cybersecurity awareness
7 platform, KnowBe4 and consists of approximately 15 minutes of general cybersecurity
8 awareness content, focused on current threats and the most up-to-date training materials
9 available. In addition, NSPI requires mandatory cybersecurity training as part of employee
10 onboarding, as well as remedial training for employees who fail a phishing simulation.

11
12 (b) Most training modules include quizzes as determined by KnowBe4. Scores are tracked and
13 retained for up to 24 months. A passing score is 80%, and employees who do not achieve
14 a passing score are required to retake the quiz.

15
16 (c) NSPI tracks 100 percent of the mandatory quarterly cybersecurity training participation,
17 with participation rates consistently around 98-99 percent. When applicable, quiz pass/fail
18 results are also documented.

19
20 **Mandatory Training:**

21

Q1 2023 – 98.6%	Q1 2024 – 99.5%	Q1 2025 – 99.3%	Q1 2026 – 100%
Q2 2023 – 99.0%	Q2 2024 – 98.6%	Q2 2025 – 98.4%	Q2 2026 – in progress
Q3 2023 – 98.7%	Q3 2024 – 98.3%	Q3 2025 – 97.9%	
Q4 2023 – 98.6%	Q4 2024 – 98.4%	Q4 2025 – 99.5%	

22
23 (d) Yes. Phishing simulations are sent to all employees every month.

24
25 New hires receive weekly phishing simulations during their first month of employment
26 after which they are enrolled in the standard monthly phishing simulations sent to all active
27 employees.

Minister of Energy – Accountability for Nova Scotia Power (NSEB M12600)
NSPI Responses to Small Business Advocate Information Requests

NON-CONFIDENTIAL

(e) Yes. NSPI tracks employee success and failure rates for phishing simulation testing exercises. Phishing simulation results are recorded and monitored within our security awareness training platform and are compared against established Balanced Score Card goals and target phishing failure rates. Summary reports are generated after each simulation and shared with NSPI leadership.

Phishing simulations are evaluated on a pass/fail basis. A failure is recorded when an employee interacts with a simulated phishing email (e.g., clicking a link or submitting credentials).

Employees who fail a phishing simulation are automatically enrolled in remedial cybersecurity training. Repeated failures are actively addressed; employees with multiple failures (two or more) are subject to additional management review and a 10% reduction to their Short Term Incentive Plan (STIP) in accordance with organizational policy.

Phishing simulation failure statistics at NSPI for the past 3 years are as follows:

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2023				2.8%	1.3%	2.3%	1.1%	4.3%	4.9%	2.3%	1.7%	11.0%
2024	0.4%	17.7%	1.7%	3.7%	1.1%	2.5%	4.7%	0.2%	0.5%	0.7%	14.3%	0.7%
2025	6.4%	3.3%	0.5%	0.2%	N/A	N/A	4.8%	1.9%	9.6%	0.5%	2.9%	1.6%
2026	1.7%	2.2%	2.8%	2.2%								

NON-CONFIDENTIAL

- 1 (f) Yes. Since the incident, Nova Scotia Power has enhanced its cybersecurity training
2 program, including onboarding phishing simulations for new hires, remedial training after
3 every failed phishing simulation (was previously after 2 failures), and strengthened
4 accountability measures tied to the STIP. A targeted five-week phishing campaign was also
5 conducted in November 2025 for employees with prior failures.

NON-CONFIDENTIAL

1 **Request IR-10:**

2
3 **Please refer to the Report, Page 18, Lines 19-29:**

4
5 **NS Power implemented a previously developed and tested consistent**
6 **multi-channel approach throughout the response efforts for all public**
7 **communications. For each update, the transparency effort involved**
8 **postings on a dedicated cyber update landing page on the Company's**
9 **website and social media channels, notice to all local media, and**
10 **communications directly to key account/business customers,**
11 **government and other stakeholders in addition to employees.**

12
13 **To ensure customers were kept informed, the Company also employed**
14 **a multi-platform paid media strategy that includes online, as well as**
15 **TV, print and radio to reach a wide variety of customer demographics.**
16 **In addition, NS Power activated a paid search strategy throughout the**
17 **Incident to ensure that the NS Power website and information**
18 **appeared as the top search result when customers used search engines**
19 **(i.e. Google) to find information about the Incident. throughout the**
20 **response efforts for all public communications...**
21

22 **(a) When was the multi-channel approach first implemented for this Incident?**

23
24 **(b) When was the paid media strategy implemented? Who bears the cost for the paid**
25 **media strategy?**

26
27 **Response IR-10:**

28
29 **(a) The multi-channel approach was implemented starting with the initial public**
30 **communication on April 28, 2025, to all customers that the company had discovered and**
31 **began actively responding to a cybersecurity incident on April 25, 2025. A record of all**
32 **dates and announcements that employed the multi-channel approach can be found at**
33 **nspower.ca.cyber.**

34
35 **(b) The paid media strategy related to the cyber incident was implemented starting on May 2,**
36 **2025, and was used in varying capacities to reach customers with urgent information**

NON-CONFIDENTIAL

1 related to the cyber incident, such as warning of an increase in scam activity and ensuring
2 that the cyber incident page of our website appeared in top search results as a trusted source
3 of information for customers. A focus on paid media continued through the end of July
4 2025. Paid media costs have been submitted and we anticipate coverage through our
5 insurance provider.

NON-CONFIDENTIAL

1 **Request IR-11:**

2
3 **Please refer to the Report, Page 19, Lines 8-9:**

4
5 **As noted above, the Company became aware of the Incident on Friday,**
6 **April 25, 2025. The next business day, on Monday, April 28, 2025, NS**
7 **Power informed customers that it was actively responding to a**
8 **cybersecurity incident and encouraged customers to report any**
9 **suspicious emails or phone calls.**
10

11 **(a) How did NS Power first notify customers?**

12
13 **(b) Was there a discussion of when to notify customers? Did NS Power receive advice**
14 **on when the notification should take place?**

15
16 **Response IR-11:**
17

18 Please see IR-1 filed with the NSEB on September 5, 2025 for details on NS Power's extensive
19 transparency efforts. On April 28, 2025, NS Power posted a communication to its website, in an
20 effort to provide broad public notice about the incident to stakeholders. The update was also posted
21 to the Company social media channels, advertised on paid media channels, as well as proactively
22 shared with and widely covered by media.
23

24 Decisions on notice to customers were made through discussions with the Company's incident
25 response team, including in conjunction with external counsel, having consideration to the
26 evolving circumstances of the incident, and the ongoing investigation.

NON-CONFIDENTIAL

1 **Request IR-12:**

2
3 **Please refer to the Report, Page 25, Lines 22-23:**

4
5 **As discussed elsewhere in this report, part of the internal process**
6 **related to this incident will include a review of lessons learned,**
7 **including a review of communications with customers.**
8

9 **(a) Will the “lessons learned” report be provided the Board and stakeholders?**

10
11 **(b) If yes, when is it expected to be completed?**

12
13 **(c) If no, why not?**

14
15 **Response IR-12:**

16
17 **NS Power will prepare a report for the Board upon completion of its incident response,**
18 **investigation, and remediation efforts (which would include accounting for the results of these**
19 **ongoing matters).**

NON-CONFIDENTIAL

1 **Request IR-13:**

2
3 **Please refer to the Report, Page 37, Lines 15-16:**

4
5 **...In connection with these efforts, NS Power has recently completed an**
6 **extensive two-year update to its cybersecurity practices to comply with current**
7 **policies and anticipated changes in standards communicated by NIST.**
8

9 **(a) When was the two-year update completed?**

10
11 **Response IR-13:**

12
13 NS Power concluded its two-year update of its cybersecurity practices spanning 2023–
14 2024, with formal closeout on February 3, 2025. NS Power regularly reviews and makes
15 continuous improvements to its cybersecurity programs to ensure it is in line with the latest
16 guidance, in addition to the update noted above.

NON-CONFIDENTIAL

1 **Request IR-14:**

2
3 **Refer to M12600, Exhibit N-1, Nova Scotia Energy Board (NESB) IR 4(a):**

4
5 **As noted above, NS Power extended the offer of credit monitoring by**
6 **three additional years beyond the two-year industry standard,**
7 **providing additional protection for delayed impacts of the breach and**
8 **made the credit monitoring available to all current and former**
9 **customers...**

10
11 **(a) Is the ‘industry standard’ referred to in the quote about referring to the electricity**
12 **industry, with respect to security breaches, or to another industry?**

13
14 **(b) How did NS Power determine the ‘industry standard’?**

15
16 **(c) At this time, is NS Power aware of any identity breaches/damages suffered by a**
17 **customer as a result of this Incident?**

18
19 **Response IR-14:**

20
21 **(a-b)** As noted the response to NSEB IR 3(g) and (h) filed with the Board on September 5, 2025,
22 a two-year time period for a credit monitoring service has become a well-established,
23 common practice for organizations across industries (financial services, healthcare, retail,
24 telecommunications, education, etc.) in North America when they suffer ransomware or
25 other data breaches involving sensitive personal information. The two-year time frame is
26 widely considered by experts to be sufficient to detect potentially fraudulent activity that
27 may arise following a cyber incident, as it provides a window for potentially affected
28 individuals to monitor their credit information, receive alerts on changes to their credit file,
29 and take steps to protect their information if needed.

Minister of Energy – Accountability for Nova Scotia Power (NSEB M12600)
NSPI Responses to Small Business Advocate Information Requests

NON-CONFIDENTIAL

- 1 (c) To date, NS Power continues to have no evidence that this information has been used for
2 identity theft, or of any financial harm to customers as a result of the misuse of the impacted
3 information.

NON-CONFIDENTIAL

1 **Request IR-15:**

2
3 **Refer to M12600, Exhibit N-1, NESB IR 6(a):**

4
5 **The Company’s investigations remain ongoing. At this time, it is not**
6 **possible to determine precisely what specific personal customer**
7 **information, if any, was affected by this incident...**
8

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

11
12 **Response IR-15:**
13

14 As outlined in the above noted response to NSEB IR 6(a), due to the nature of the breach and the
15 complexity of the systems involved, and despite the Company’s comprehensive investigative
16 efforts, it is the case that the data accessed or exfiltrated cannot be definitively identified with
17 confidence on an individual basis. There is no expectation that this assessment will change.

NON-CONFIDENTIAL

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.

Response IR-16:

(a) See Section 8.5 of the Incident Report for detail on NS Power’s historical practices relating to the collection, use and disclosure of customer SINS.

For clarity, in 2019, based on the available information, NS Power’s practice was no longer to collect social insurance numbers (SINs) from customers, and employees were instructed to delete any customer social insurance numbers (SIN) on a reactive basis when they encountered them in the customer information system (CIS).

NS Power later commenced efforts to develop a proactive process to remove SINS from the CIS with the assistance of technical tools. The deployment of this process commenced

NON-CONFIDENTIAL

1 in 2024. The development and execution of this process was complex due to the CIS's
2 integration with multiple back-end legacy platforms and processes that underpinned
3 various existing business procedures.

4 (b-c) Due to the complexity of the systems, and variety of processes and systems involved, as
5 well as the nature of the structure of the data, it is not possible for NS Power to determine
6 how many SINS were removed through these processes.

1 **Request IR-17:**

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

4
5 **...Also, the Company has not applied late charges, or penalties on any**
6 **outstanding balances since the incident. NS Power will communicate**
7 **directly with customers before reintroducing late fees on outstanding**
8 **amounts.**
9

10 **(a) Does NS Power know when it expects to reinstate late fees?**

11
12 **(b) Is there any financial impact on NS Power for waiving late fees? If so, what is the**
13 **current estimate of that impact and who bears it?**

14
15 **Response IR-17:**

16
17 a) NS Power has not finalized the exact date of communication, but appropriate advance
18 notice will be provided to customers before late fees are reinstated.

19
20 b) Late fees are recorded in Other Revenue in NS Power's Financial statements. NS Power
21 collected \$[REDACTED] less in Late Fees in 2025 compared to the expectation in the 2025 Budget.
22 Lower revenue for NS Power results in lower earnings, which causes a reduction in NS
23 Power's regulated return on equity, therefore NS Power bears the financial impact.

NON-CONFIDENTIAL

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?**

Response IR-18:

- (a-b) See Section 4.1 of the Incident Report provided to the Board for a description of the existing cybersecurity safeguards employed by NS Power at the time of the Incident, which included protections and controls relating to endpoint detection and response, anti-malware, privileged access management, firewalls with intrusion prevention, network detection and response, data loss prevention, web filtering, email protection, vulnerability management, application security testing, and dark web monitoring.**

NON-CONFIDENTIAL

- 1 (c) NS Power has provided detail on the steps that it has taken to enhance its cybersecurity
2 environment to facilitate the prevention of future breaches in the wake of the Incident in
3 Section 8.1 of the Incident Report (and subsequent monthly updates).

NON-CONFIDENTIAL

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?

Response IR-19:

The incident did not impact all NS Power’s systems, and there remain backup systems that were not impacted. However, with respect to the systems impacted in the incident (which impacted only NS Power’s information technology network), these systems were not recoverable from a current backup, except for certain backups from an earlier currency:

- the HR Peoplesoft system, for which an old tape backup from 2023 was found to still be readable and useable;
- SharePoint from an April 24, 2025 backup; and
- the network drives up to Dec 31, 2023.

NS Power’s recovery efforts have included leveraging these secure backups to restore, and where necessary, rebuild core business applications and infrastructure.

REDACTED

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?

Response IR-20:

See the Incident Report, Section 4.3.

As noted in previous reports, after becoming aware of the Incident on April 25, 2025, NS Power commenced a thorough investigation with the assistance of external experts to determine the scope of the incident, including its impact to personal information. Based on these investigative efforts, on May 1, 2025, NS Power determined that customer information had likely been impacted in the Incident. Its investigation remained ongoing to determine the nature and extent of the impacted data.

On May 4, 2025, in the course of ongoing confidential interactions with the threat actor (conducted through a third party threat actor negotiation firm), the threat actor provided the Company with [REDACTED] (the [REDACTED])

REDACTED

1 “proof” provided by the threat actor referenced in the Compliance Letter). This file tree list
2 contained directories of data, which included customer information.

3 On May 22, 2025, NS Power became aware that the threat actor had published data on the dark
4 web, upon receiving communications from the threat actor that included a hyperlink to an unlisted
5 page accessible through the Tor network on the dark web, and promptly provided an update to
6 customers through the same channels as previous updates, including updating the company’s
7 website and social media channels, notifying local media, and conducting media interviews.

8 As noted in the OPC Compliance Letter referenced above, to date, other than the posting of the
9 data on the dark web by the threat actor, there has been no indication of misuse of the data accessed
10 by the threat actor, and the Company has not become aware of any additional information or
11 instances that provide evidence that any customer’s personal information has been misused in a
12 manner that is directly connected to this Incident. As noted in the Compliance Letter, there is no
13 evidence that the data obtained by the threat actor has been made public or sold.