Nova Scotia Energy Board

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

M12273

Board Inquiry into Nova Scotia Power's Cybersecurity Incident

Nova Scotia Power
Incident Report

December 22, 2025

REDACTED

TABLE OF CONTENTS

1.0 INTRODUCTION

In its July 14, 2025 letter regarding the cybersecurity incident (Incident) experienced by Nova Scotia Power Inc. (NS Power, Company), the Nova Scotia Energy Board (NSEB, Board) advised that "the Board will require a report from NS Power about the incident"[1] and that "[t]he 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."[2] The NSEB noted that the Incident report should include several categories of information,[3] as follows:

- Incident Description
- Affected Systems and Data
- Indicators of Compromise
- Root Cause Analysis
- Impact Analysis
- Response and Recovery Actions
- Collection and Retention of Personal Information
- Recommendations

On November 7, 2025, the NSEB provided additional direction as follows:

1. Settle any outstanding dues of vendors or suppliers as soon as possible, and in the January monthly report, indicate what percentage of invoices remain pending, along with an aged analysis of the payables and the reasons for the accounts outstanding beyond 30 days. The Board will also refer this matter to MNP to further investigate causes of the NS Power's financial technology data compromise and assess its data handling practices.

[1] M12273, Board Inquiry into Nova Scotia Power's Cybersecurity Incident, NSEB Letter, July 14, 2025, page 1.
[2] M12273, NSEB Letter, July 14, 2025, pp. 2-3.
[3] M12273, NSEB Letter, November 7, 2025, pp. 1-2.

2. In the incident report to be filed by the end of this year, please provide a Gantt chart that includes a list of all the summary tasks/rolled-up tasks currently undertaken to achieve full recovery. The chart should specify the expected completion time, start date, finish date, and percentage completion. If no progress is made from one month to the next, this should also be clearly indicated along with the reasons.

3. A separate chart is to be provided in the Incident Report which includes the list of Board matters or potential proceedings which are impacted and a forecast date for the restoration of normal activities in each matter.[4]

In accordance with the Board's direction, this report provides the information requested. This report also provides a Gantt chart of systems restorations timelines and another chart with a list of impacted Board matters and proceedings. Please refer to Appendices A and B, respectively. With respect to the NSEB's direction regarding outstanding dues to vendors and suppliers, the Company is working to compile this information and anticipates being in a position to provide the requested information to the Board in early February 2026.

On December 3, 2025, the Premier of Nova Scotia issued an open letter to the NSEB regarding the Incident. The Premier called on the Board to launch a formal investigation into:

1. The fairness and legality of NSP's estimated billing methodology.
2. The adequacy of consumer protections and communication during this period.
3. The timeline and contingency planning for restoring accurate billing systems.
4. Whether NSP should provide financial relief, credits, or bill smoothing options to affected customers.
5. Whether NSP is subject to financial penalties; and if so, the maximum amount that can be levied.[5]

[4] M12273, NSEB Letter, November 7, 2025, p. 2.
[5] M12600, Minister of Energy – Accountability for Nova Scotia Power Inc., Minister of Energy Letter, December 3, 2025.

The NSEB replied to the Premier by letter on December 10, 2025, providing, in part, the following:

> Upon receipt of your letter, the Board opened a new matter (M12600). Given the connection between these issues and the Board's ongoing inquiry into the cybersecurity incident (M12273), the Board will consider whether the issues raised in your letter would be most effectively and efficiently addressed in a separate proceeding or in the ongoing cybersecurity inquiry.
>
> //
>
> The Board anticipates scoping the necessary additional processes for the cybersecurity matter upon receipt of the utility's formal report later this month. The content of the report and the responses to the Board's outstanding information requests will inform whether the issues outlined in your letter would be most appropriately addressed in the cybersecurity matter or separately in the new matter.[6]

The Company notes that many of the issues raised by the Premier, specifically the estimated billing, customer communications, timelines and contingency planning for restoration of normal billing, and customer assistance programs, were addressed in the monthly Incident update report for November provided by NS Power on December 1, 2025, with additional details provided herein. Finally, the Board's second set of Information Requests (IR) received under this matter on December 3, 2025, deal specifically with the customer billing issue. Responses to those IRs are due to the NSEB on December 23, 2025. Accordingly, NS Power believes that M12273 is the appropriate proceeding in which to address the issues raised by the Premier without the need for a new matter.

On December 10, 2025, the NSEB provided additional direction by letter stemming from a customer complaint (M12457). In its letter, the NSEB noted as follows:

> At this stage, the Board requires that NS Power report back on the progress made and outcomes of this broader review. As this review involves broader issues than that of the complainant, it is appropriate that the update be provided in a separate process from the initial complaint. The Board would, therefore, request that NS Power include information on the progress made on this issue in the final report in

[6] M12600, NS Power Letter, December 10, 2025, p.1.

Matter M12273-Board Inquiry into Nova Scotia Power's Cybersecurity Incident. This would be the most efficient way to address the matter.[7]

Accordingly, the Board's directive is addressed in this report.

[7] M12457, NSPI Complaint – Systemic Regulatory Compliance Issues – Blarney Stone Restaurant, NSEB Letter, December 10, 2025.

2.0 THE INCIDENT

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the Incident:

- A detailed account of how NS Power discovered the breach.
- A description of the attack vector.
- A timeline of events from detection to resolution.[8]
- 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.[9]
- A description of how the breach occurred.
- An identification of vulnerabilities or security gaps that were exploited.[10]

NS Power addresses each in this section.

Discovery of the Breach and Background

The Incident involved a sophisticated and coordinated criminal cyberattack on certain of NS Power's information technology systems and data.

The Incident was discovered on April 25, 2025, when NS Power employees reported certain applications on the Company's systems were not functional. Upon immediate investigation, it became evident that a threat actor had gained unauthorized access into certain parts of NS Power's information technology network and servers which support portions of its business applications.

[8] M12273, NSEB Letter, July 14, 2025, p. 1.
[9] M12273, NSEB Letter, July 14, 2025, p. 1.
[10] M12273, NSEB Letter, July 14, 2025, p. 2.

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.

Under the direction of Osler, Mandiant assisted the Company and other cybersecurity experts with containment, investigation, and remediation efforts, and took immediate actions to contain and remediate the unauthorized activity, including containing and isolating affected servers, limiting network connectivity, identifying and resetting compromised account credentials, and hardening the environment. Teams within NS Power also began working diligently with cybersecurity experts to further isolate the operational technology and energy delivery systems.

The Company continues to have no evidence the threat actor accessed any operational technology or energy delivery systems.

Based on the investigation, the Company believes that an unauthorized third party gained access on or around March 19, 2025 and, beginning on or around April 25, 2025, exfiltrated certain data, including personal information of the Company's customers.

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. Given the nature of the cyber attack, the critical infrastructure nature of the company and the North American electric utility industry, and the high confidence our advisors had of the identity of the threat actor, the Company also notified the Federal Bureau of Investigation (FBI).

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. The OPC initiated an investigation into the Incident, on May 28, 2025 and the Company is actively and fully cooperating with the OPC to support the OPC's investigative efforts.

Incident Timeline & Attack Vector

The forensic investigation of the Incident has been complex.

[redacted]

The date of initial compromise of the Company's systems was determined to be March 19, 2025.

[redacted]

[redacted]

On April 25, 2025, NS Power disabled external access to the NS Power environment, and began to isolate systems with suspicious or malicious activity.

[redacted]

The Incident has not caused any disruption to physical operations at NS Power's generation, transmission and distribution facilities, and the Incident has not impacted the Company's ability to safely or reliably provide electricity to customers in Nova Scotia.

3.0 AFFECTED SYSTEMS AND DATA

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the affected systems and data:

- An identification of compromised systems and data.
- Specific details about the type and amount of personal information exposed.[11]

NS Power addresses each in this section.

3.1 Compromised Systems

NS Power has previously described affected systems in its October 1, November 3, and December 1, 2025 monthly Incident update reports, under the Incident Impact and Response section. Those systems include, broadly:

- Enterprise Resource Planning (ERP) systems:
  - PeopleSoft
  - PowerPlan
  - Oracle E-Business Suite

- Customer Billing and Customer Systems:
  - MyAccount
  - Advanced Metering Infrastructure Head End System
  - Backup Advanced Distribution Management System
  - MV90
  - Packaged Contact Center Enterprise

[11] M12273, NSEB Letter, July 14, 2025, p. 1.

- Additional systems:
  - Aligne Fuels/Plant Information (PI)
  - Geospatial Information System
  - Adept Restoration
  - Certain Laptop Computers
  - Self-Serve Business Intelligence & Analytics
  - [redacted]

- Cybersecurity systems and tools:
  - Active Directory
  - Privileged Access Management Tool
  - Security Information and Event Management Tool
  - Vulnerability Management Tool
  - Public Key Infrastructure System
  - Data Classification and Data Loss Prevention Tools
  - Mobile Device Management Tool

- Data Centre Technology:
  - Servers & Virtual Environment
  - Network & Firewall Infrastructure
  - Backup Systems
  - Network Attached Storage (NAS)
  - SharePoint File Storage

Please also refer to Appendix A which provides the above noted list of affected technology systems, and Gantt chart illustrating restoration progress to date and timelines.

3.2 Data & Personal Information

[redacted] The process to identify the customers who were directly impacted has been extremely complex, and has been completed. As set out in the notices sent to impacted customers, the impacted data would have varied by customer, and depended, in part, on the information a customer would have provided NS Power (i.e. not all personal information elements would have been impacted for all notified customers).

The Company stated in its notice to impacted customers that the unauthorized third party gained access to various types of personal information of customers that included the following: name, phone number, email address, mailing and service addresses, NS Power program participation information, date of birth, and customer account history (such as power consumption, service requests, customer payment, billing, and credit history, and customer correspondence), driver's license number, and social insurance number (SIN). For some customers, bank account numbers (for pre-authorized payment) may also have been impacted, if this information was provided by these customers. With respect to direct notifications, the Company issued two versions of notification letters to impacted customers. The letters were substantively identical, except that one version advised the customer that based on the investigation, their social insurance number may have been affected by the Incident.

4.0 RESPONSE AND RECOVERY ACTIONS

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the 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.[12]

NS Power addresses each in this section. Please also refer to Section 2 above.

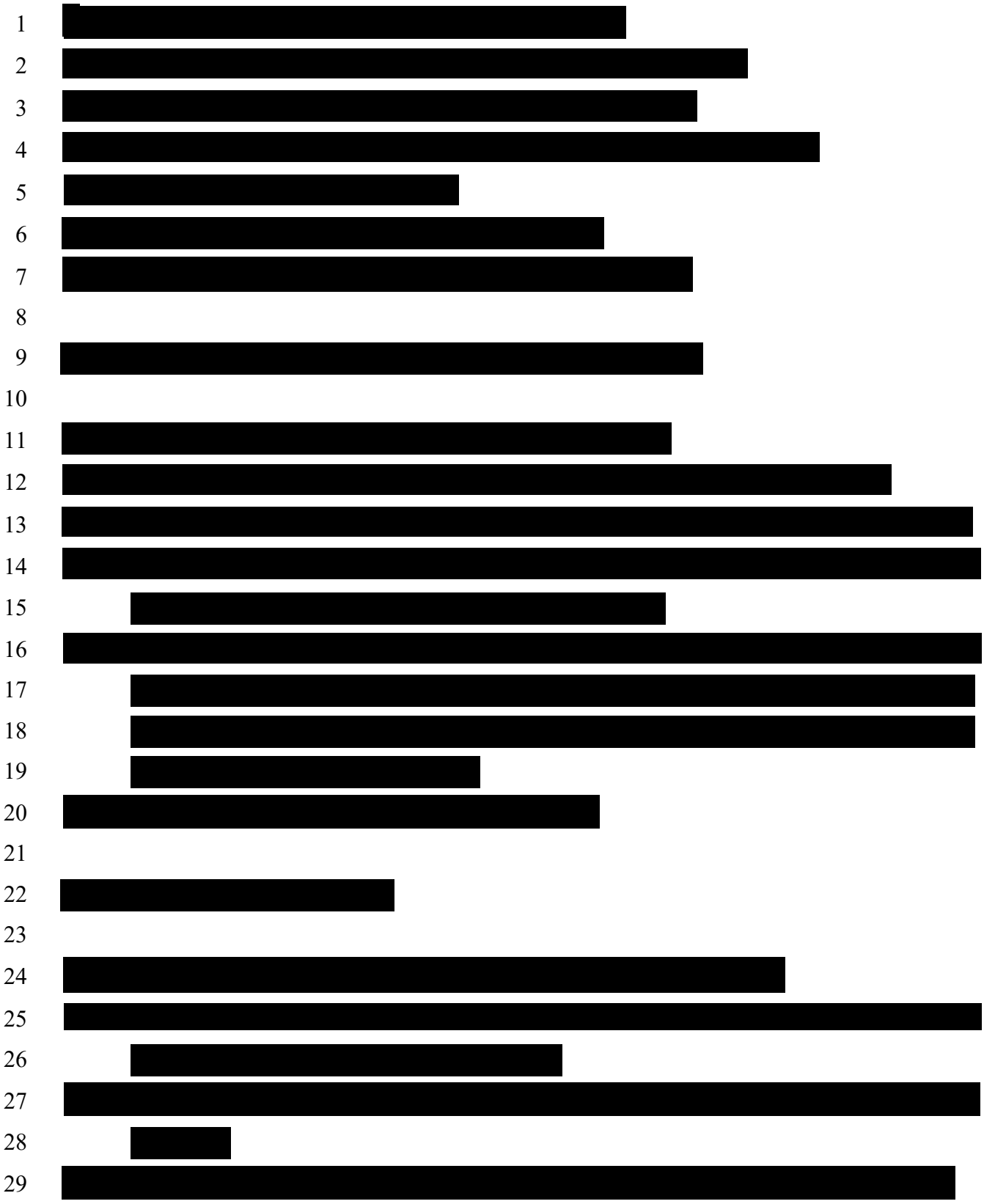
4.1 Mitigation and Restoration Actions

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.

Immediate remediation actions were taken:

[12] M12273, NSEB Letter, July 14, 2025, p. 2.



[redacted]

NS Power is also advancing efforts to restore and, where necessary, rebuild core business applications and infrastructure — including finance, human resource, procurement, certain customer billing systems, and integrations between those systems and other supporting systems — by leveraging secure backups and reestablishing security and monitoring protocols across systems. These recovery efforts are focused on ensuring continuity and stability for the Company's business operations and customers.

To coordinate work streams on business restoration and information security strengthening efforts, a business restoration process office (RPO) has been established within NS Power. Restoration efforts are continuing, and [redacted]

Key additional remediation and restoration efforts related to strengthening the Company's cyber security systems include:

[redacted]

Existing Safeguards

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. 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.

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.

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.

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.

4.2 Communications to Customers

Customer Communications and Response

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.

The Company's robust transparency effort is evidenced by the public communications that NS Power has engaged in throughout the Incident.

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. This paid search strategy was also used to reduce the risk of fraudulent activity related to searches for the

official Nova Scotia Power website. Social media accounts have been regularly updated and monitored, and where appropriate, the Company has provided answers to related customer questions online. Customers were also able to speak directly with NS Power customer care representatives on the phone throughout the Incident for any questions or concerns.

Customer Notification Timeline

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.

On May 1, 2025, NS Power determined that customer information had been impacted in the Incident, and promptly updated customers using the multi-channel strategy noted above to inform them that they had identified that certain customer personal information had been impacted in the Incident, and again encouraged them to remain vigilant and cautious of unsolicited communications and potential scams. The Company informed customers that they were working urgently to determine the full nature and scope of the data that may have been affected. The Company also initiated the process of notifying affected individuals, including retaining third-party service providers to assist with this effort.

[redacted]

On May 13, 2025, NS Power sent direct notices to approximately 277,000 current customers whose personal information the Company was able to determine had been impacted in this incident.

The following morning (May 14, 2025), the Company also issued a press release, provided a detailed update on its website, and updated its various social media accounts, which received widespread coverage in the local and national media. Senior Company personnel, including the President & CEO, participated in multiple media interviews to ensure that the public remained informed about the Incident.

NS Power's notice to impacted customers also included guidance 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 credit monitoring service offered to customers is provided by TransUnion and has been specifically designed to protect individuals in the case of a data breach, and offers them access to the following protective features:

- Unlimited online access to their TransUnion Canada credit report, updated daily, which offers individuals access to the individual's financial history and is one of the primary tools leveraged for determining credit-related identity theft or fraud.

- Unlimited online access to their credit score, updated daily.

- Credit monitoring, which provides individuals with email notifications to key changes on an individual's TransUnion Canada credit report. These credit alerts help protect individuals against identity theft, enable quick action against potentially fraudulent activity and provide them with additional reassurance.

- Access to online educational resources concerning credit management, fraud victim assistance and identity theft prevention.

- Access to Identity Restoration agents who are available to assist individuals with questions about identity theft. In the unlikely event that an individual becomes a victim of fraud, a personal restoration specialist will help to resolve any identity theft.

- Up to $1,000,000 of expense reimbursement insurance related to identity theft.

- Dark Web Monitoring, which monitors surface, social, deep, and dark websites for potentially exposed personal, identity and financial information and helps protect individuals against identity theft.

Thereafter, NS Power continued to keep customers updated regarding the ongoing incident and investigation through updates on its website landing page dedicated to cyber updates.

On May 22, 2025, NS Power became aware that the threat actor had published data on the dark web, and promptly provided an update to customers through the same channels as previous updates, including updating the company's website and social media channels, notifying local media, and conducting media interviews.

Former Customers

As the Company continued its investigation of the impacted data, NS Power determined that personal information relating to former customers had also been impacted by the Incident.

On June 25, 2025, NS Power notified the public that information related to former customers had also been impacted in the Incident. In addition, out of an abundance of caution, and in the interest of assisting customers further to mitigate the potential harm to current and former customers arising from the Incident, NS Power proactively extended the credit monitoring offer to five years for all current and former customers. Customers who had already registered for credit monitoring had their monitoring timeframe automatically extended.

Given that NS Power does not have updated contact information for its former customers, the Company worked to share this indirect notification as broadly as possible. In addition to its website, NS Power actively shared this information with media, on social media, with stakeholders, through paid advertising, as well as national paid search optimization, to reach as many current and former customers as possible.

Additional Customer Notification

NS Power has continued its investigation into the scope and nature of the impacted data with the assistance of leading third-party data analysis experts to determine the precise number of impacted individuals. This was a highly complex and time-consuming exercise, which included using data discovery tools, and extensive manual review.

As a result of these efforts, Nova Scotia Power identified approximately 97,000 additional customers who were impacted in this incident. Nova Scotia Power sent direct notices to these individuals on October 31, 2025, and offered them an additional opportunity to sign up for credit monitoring, to the extent they have not already done so.

In sum, at this time, Nova Scotia Power has sent direct notifications to approximately 375,000 customers who have been identified as being impacted in this incident.

Customer Support for Credit Monitoring and Dedicated Call Centres

Promptly upon becoming aware of the Incident, NS Power established a dedicated call centre where individuals could receive more information about the Incident, and support for credit monitoring sign-ups, whose number was included in the notice letters and made available to customers.

As is standard in incidents of this nature, to ensure that the call centre had sufficient capacity to handle the volume of calls and allow NS Power's customer service team to focus on a subset of

escalated queries, this call centre was staffed by TransUnion employees who had been provided with prepared responses from NS Power, and instructed to escalate any queries that could not be addressed to the Company so that customers could receive a call-back from the NS Power customer service team. This also allowed customers to connect directly with TransUnion for assistance in signing up for credit monitoring (and a dedicated phone line for questions about the credit monitoring process was included with the instructions provided to customers in their letter).

Having TransUnion operate the call centre enabled flexible staffing to accommodate the initial high volume of calls, and reassignment of call centre staff as call volumes dropped.

Where a customer requested a call back or had questions that could not be answered by the prepared information provided to the call centre staff, a list of customer call back requests, with relevant information, was provided to NS Power on a daily basis, whose customer care team would reach out to these customers.

To assist current and former customers with the sign-up process, the Company deployed dozens of employees to communities across the province to provide hands-on support for customers who prefer assistance in person, recognizing that not all customers may be comfortable registering online, and to ensure that customer needs are being met and access to services was being provided. More than 30 of these community sessions were held, assisting over 700 customers in signing up for the credit monitoring service. Our focus on community engagement sessions builds on NS Power's approach over the past two years where we regularly engage with customers on reliability and other customer topics of interest.

In addition, the NS Power website was updated with additional tips and tools to help customers navigate support services and a fact sheet was created with information about the service and tips for signing up. This guidance also included information on additional measures customers could take to protect themselves against identity theft. Thousands of paper copies were distributed and available to customers across the province through the customer support sessions at community locations. In addition, the fact sheet was available at NS Power local depots and provided to MLAs

and local councilors' offices. NS Power has actively encouraged customers and its employees to reach out to their family and neighbours to encourage them to sign up.

Customer Support for Bills

NS Power acknowledges and understands customer concerns with the estimated billing process.

When billing resumed in June, NS Power created a dedicated webpage at nspower.ca/billing to outline the billing process and options available for customers. Since that time, the company has included three separate inserts with customer bills to communicate information regarding the impacts of the Incident on billing, and the need to estimate bills and adjust them once meters are read either physically or data is able to be retrieved remotely. These bill inserts have also all included notice of and direction to the website content. NS Power also informed customers of the improvements made to the online customer portal (My Account) including new features and information on updated login screens for better security and user experience.

NS Power will continue to revise bill insert content to reflect the current customer experience and options, including further promotion of the ability for customers to submit a photo of their meter. With the challenges related to estimated billing causing concerns for customers, Nova Scotia Power is also holding a series of in-person community sessions across the province to answer questions and help customers understand the options related to their bills. These sessions are promoted through local media (including radio and TV), shared with local government and other stakeholders, and published on the homepage of the company's website. In December 2025, sessions have been held in Yarmouth, Port Hawkesbury and Truro, helping dozens of customers with their bills. Additional sessions, originally scheduled for December but postponed due to inclement weather, are scheduled for January 2026 in Sydney and Middleton. A list of upcoming dates can be found at nspower.ca/billing.

Ongoing Customer Communications Efforts

As discussed above, NS Power has been committed to transparency in its communications with customers and other stakeholders throughout the cyber response to date. This approach has focused on the importance of sharing known information in a timely and transparent matter, without speculating on information yet to be confirmed by the investigation into the cyber incident.

Nova Scotia Power's communications response and approach to the cyber incident, and the subsequent need to communicate with customers about estimated billing has and will continue to evolve based on availability of new information, customer feedback, and as systems continue to be restored. As the issue has progressed, Nova Scotia Power has been able to share more specific information with customers and stakeholders across more channels. In-person sessions in rural communities are a key example of this, as is the use of paid ads on both rural and urban radio stations to reach customers who may not use digital modes of communication. Building on the success of community information sessions related to reliability, the company has held sessions to assist customers with the sign-up process for credit monitoring and more recently to help customers understand their options related to estimated billing. Feedback from customers at these in-person sessions, as well as customer feedback received through digital channels and the Customer Care Centre continue to shape the information the Company is providing and the channels the Company is using to ensure customers have the information they need.

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.

4.3 Other Stakeholders

NS Power employees have been a key stakeholder audience throughout the Incident, as they were impacted as employees and as customers. Employees have received ongoing communications in the form of emails, in-person updates from senior leadership and from direct supervisors throughout the response and restoration to date. Ahead of each public update related to the cyber

investigation, employees were made aware of the latest information and what to expect in terms of public information, increased media coverage, and senior officials appearing before various provincial government committees. Where appropriate, employees were provided with Frequently Asked Questions (FAQs) to help answer their questions and help employees answer questions they were receiving from friends and family who are also customers of NS Power. In addition to updates related to the cyber response itself, employees were regularly updated about payroll, as the Company worked to restore payroll systems impacted by the Incident.

Due to the high volume of employee communications being shared in the early stages of response and restoration, a weekly summary email of all employee communications provided that week was also developed and shared with employees during the early stages of the Incident. As the Company's internal communications portal was impacted by the Incident and no longer available as a repository for employee updates, the Company established a new SharePoint site, accessible to all employees. This site continues to function as a key information resource for employees looking to read the latest update and find answers to FAQs.

As part of NS Power's communications to customers and stakeholders, additional key interest groups were also kept informed of key updates and milestones during the cyber response and investigation effort. These stakeholders included Efficiency Nova Scotia/E1, The Clean Foundation, the Independent Energy System Operator – Nova Scotia, representatives of the Affordable Energy Coalition, and key contacts within Nova Scotia's Mi'kmaw communities.
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.

As noted above, 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. Given the nature of the cyber attack and the critical

infrastructure nature of the company and the North American electric utility industry, the Company also notified the Federal Bureau of Investigation (FBI).

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.

4.4 Response Analysis

The Company considers that its response to the incident—encompassing containment, remediation, and investigation—was effective and executed in a very timely and highly coordinated manner, having regard to the severity and complexity of the attack.

The Company attributes the effectiveness of its response primarily to preparatory measures that were in place prior to the Incident, including:

- the advance engagement and retention of experienced third-party cybersecurity and incident-response experts, which ensured their immediate availability once the incident was identified;
- reliance on high-caliber external expert advice and technical expertise throughout the response and investigation;
- regular review and updating of incident-response plans and playbooks in advance of the Incident; and
- the conduct of repeated tabletop and simulation exercises, which helped ensure that personnel were familiar with their respective roles and responsibilities and supported an orderly and efficient execution of response activities.

During the Incident response, governance structures and workstreams were clearly established, and appropriately experienced and skilled subject-matter experts and decision-makers were engaged from the outset. This facilitated timely escalation, prioritization of actions, and coordinated decision-making. Internal communication and coordination among executive

leadership, relevant business units, and the Incident-response team functioned very effectively throughout the Incident response period.

At the same time, the Company recognizes—as a matter of sound governance and consistent with industry practice—that even an effective incident response will identify areas for refinement. The Incident has provided NSP with valuable, practical, real-world insights that could not have been fully replicated through planning or exercises alone.

Accordingly, and irrespective of its assessment of the effectiveness of the response, the Company is treating the Incident as a learning exercise to further strengthen its preparedness and resilience.

Areas of focus for continuous improvement include:

- updating incident-response plans and playbooks to reflect observed, real-world conditions;
- incorporating incident-specific lessons and scenarios that are difficult to anticipate fully through tabletop exercises; and
- enhancing documentation to improve repeatability, training, and the Company's institutional knowledge for future responses.

The Company considers this continuous improvement approach to be an essential component of responsible cybersecurity governance.

5.0 COLLECTION AND RETENTION OF PERSONAL INFORMATION

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the 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.[13]

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. In the wake of the Incident, NS Power is working to enhance its overall privacy governance framework and build on its existing privacy program (policy, procedures and standards) by taking the following actions:

- Ensuring the Company's privacy officer who, along with the privacy committee, will be responsible for:
  - clarifying expectations for all NS Power employees relating to data and privacy protection and cybersecurity and enhancing privacy training
  - enhancing the operationalization of the privacy program; and
  - further promote a culture of privacy and risk-based decision-making, where employees are encouraged to escalate and report privacy issues and there are clear reporting processes in place.

[13] M12273, NSEB Letter, July 14, 2025, p. 2.

6.0 IMPACT ANALYSIS

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the 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.[14]

NS Power addresses each in this section.

6.1 Impact

NS Power financial and internal operational impacts noted by the Board above have been reported in the Company's monthly Incident update reports and in the preceding sections, as well as our publicly available financial statements. Please also refer to **Appendices A** and **B** for a list of systems affected and affected regulatory matters, respectively. As noted above, with respect to the operation of the grid, the Company continues to have no evidence the threat actor accessed any operational technology or energy delivery systems. Core operations and the electric grid continued uninterrupted – no power was lost to Nova Scotians.

NS Power is aware of the concerns this incident has caused for customers and is committed to restoring trust with its customers. Peter Gregg addressed this in his opening statement to the Standing Committee on Natural Resources and Economic Development on November 25, 2025:

[14] M12273, NSEB Letter, July 14, 2025, p. 2.

> At Nova Scotia Power, our commitment to providing reliable power to Nova Scotians has been unwavering for over 100 years. We recognize that the recent cyber event has affected the trust we have built with our customers, and I want to acknowledge and apologize for the concern and disruption this has caused.
>
> Over the past 215 days, our team has worked around the clock to restore and strengthen our systems and to support our customers. And we recognize that the cyber incident continues to impact our customers, including concerns about estimated bills. To you the committee, and to all Nova Scotians, my promise to you is if we have overestimated your bill, we will fix it. If you have overpaid, we will fix it. And if we make a mistake, we will fix it.
> //
> Most importantly we remain focused on the impact this has had on Nova Scotians. We understand the ongoing challenges related to billing, payments to our suppliers, and longer wait times to speak with our care team, and we are working diligently to resolve them. Restoring all systems will take time, but we are providing flexible options for our customers – such as equal billing, pay-what-you-can arrangements, and photo meter reads – until we're able to reconnect our systems and provide up-to-date bills.
>
> 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. We are also on track to reconnect customer meters with our billing systems by the end of March. Our team has worked to address outstanding payments to suppliers, and we expect to be caught up on these payments before the end of the year.
> //
> In closing, I want to reiterate our commitment to supporting Nova Scotians, minimizing the impact of this incident, and rebuilding trust. We do not take this responsibility lightly. Again, my promise to you is if we have overestimated your bill, we will fix it. If you have overpaid, we will fix it. And if we make a mistake, we will fix it.[15]

Please also refer to section 4.2 above for full details on how NS Power is addressing impacted customers and their concerns.

[15] Peter Gregg, President & CEO, Nova Scotia Power, Opening Statement to the Standing Committee on Natural Resources and Economic Development, November 25, 2025.

6.2 Assessment of Potential Harm

As outlined above, NS Power determined through its investigation that certain customer information stored on the impacted servers was accessed and taken by an unauthorized third party. However, while NS Power recognizes the potential impact the Incident may have had on customers, Nova Scotia Power continues to have no evidence that this information has been further misused, or of any financial harm to customers resulting from this Incident.

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, as described in detail above in Section 4.2. The Company's objective throughout has been to provide affected individuals with meaningful support, reduce the risk of harm, and maintain trust.

As also noted above, the Incident has not caused any disruption to physical operations at NS Power's generation, transmission and distribution facilities, and the Incident has not impacted the Company's ability to safely or reliably serve customers in Nova Scotia.

The Incident caused a severe, adverse impact on the Company's billing systems, and NS Power recognizes that concerns have been raised about the Company's estimated billing process. The Company is treating these concerns very seriously. In the immediate response to the Incident, NS Power committed and confirmed that customers would not be charged late fees or have their service disrupted as a result of this Incident. NS Power is committed to addressing these impacts, and to alleviating the concern and disruption it has caused customers. NS Power has never intentionally overbilled its customers and has been steadfast and consistent in its commitment to customers that it is actively trying to address the issues and, where mistakes have been made, they will be fixed.

NS Power continues to work with customers to offer payment options. The Company encourages any customers who have concerns to call the Customer Care Centre. Restoring all systems will

take time, but the Company is providing flexible options for customers—such as Equal Billing, pay-what-you-can arrangements, and photo meter reads—until NS Power is able to reconnect the systems and provide up-to-date bills.

7.0 M12457 DIRECTION

As noted in the introduction, the NSEB directed NS Power to address the broader review outcomes arising from M12457. Each of the Board's questions are addressed in turn in Appendix C.

8.0 RECOMMENDATIONS

In its letter of July 14, 2025, the NSEB directed the following be included in the Report regarding the 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.[16]

Each is addressed in turn below.

8.1 Enhancing Security Measures and Preventing Future Breaches

NS Power has taken the following steps to enhance its cybersecurity environment to facilitate the prevention of future breaches:

[redacted]

[16] M12273, NSEB Letter, July 14, 2025, p. 2.

8.2 Additional Security Audits, Policy Updates, and Employee Training

Section 4.1 addressed additional security audits, policy updates, and employee training as summarized below.

Regarding security audits, NERC conducts extensive periodic audits (including security) of the Company's Energy Operations to ensure effective compliance. In addition, as noted in the Company's Incident monthly updates, the Office of the Privacy Commissioner of Canada (OPC) has initiated an investigation into the Incident, which remains ongoing. The Company continues to fully cooperate with the OPC and remains committed to addressing the OPC's concerns and resolving the investigation in an efficient and expeditious manner.

Regarding policy updates, NS Power had implemented a common set of cybersecurity standards and policies that are informed, in part, by the 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. 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.

Regarding employee training, 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.

8.3 New Strategies and Proactive Measures

With respect to new strategies and proactive measures, please refer to section 8.1 above.

8.4 Customer Communications

With respect to improving communications and responsiveness to the concerns and needs of NS Power's impacted customers, as noted in section 4.2 above, 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.

NS Power took the following actions:

- Conducted a consistent multi-channel public communications approach throughout the response efforts.
- Conducted a multi-platform paid media/advertising strategy.
- Implemented 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.
- Updated and monitored social media accounts and, where appropriate, provided answers to related customer questions online.
- Provided customers the ability to speak directly with NS Power customer care representatives on the phone and via email throughout the Incident for any questions or concerns.
- Notified affected individuals, including retaining third-party service providers to assist with this effort.
- 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 25, 2025. Customers who had already registered for credit monitoring had their offer automatically extended.

- Established a dedicated call centre where individuals could receive more information about the Incident, and support for credit monitoring sign-ups, whose number was included in the notice letters and made available to customers.
- Staffed this call centre with TransUnion employees who had been provided with prepared responses from NS Power and instructed to escalate any queries that could not be addressed to the Company so that customers could receive a call-back from the NS Power customer service team.
- Provided guidance on registering for credit monitoring posted online and made available in locations throughout the province.
- Created a fact sheet with information about the service and tips for signing up.
- Distributed and made available thousands of fact sheet paper copies to customers across the province through customer support sessions at community locations. In addition, the fact sheet was available at NS Power local depots and provided to MLAs and local councilors.
- Deployed dozens of employees to communities across the province to provide hands-on support for customers.
- Updated the NS Power website and social media channels also with additional tips and tools to help customers navigate support services.

NS Power continues to keep customers updated regarding the ongoing incident and investigation. In summary, at this time, Nova Scotia Power has sent direct notifications to approximately 375,000 customers who have been identified as being impacted in this incident.

8.5 Collection and Retention of Personal Information

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.

As described in Section 5, in the wake of the Incident, NS Power is working to enhance its overall privacy governance framework and build on its existing privacy program.

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."[17]

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.

In limited circumstances, NS Power continued to collect SINs from customers where there was a legal requirement to do so. SINs continued to be collected for tax reporting purposes where NS

[17] Peter Gregg, President & CEO, Nova Scotia Power, Opening Statement to the Standing Committee on Natural Resources and Economic Development, November 25, 2025.

Power was required to issue a T5 in connection with interest over $50 earned in a year on a customer deposit.

In 2021, Nova Scotia Power initiated a customer energy management program called MyEnergy Insights to better inform customers of their energy usage patterns. The MyEnergy Insights program required a daily export of customer information from NS Power's CIS into a staging area within NS Power's Azure environment (cloud storage environment). Within this staging area, certain daily exports from July 2021 were targeted by the threat actor for exfiltration. It is important to note that all data within the Azure environment was (and is still) encrypted at rest with only approved users having authorized access to that environment. Based on the investigation, the Company believes that the data exported to the Azure staging area for the MyEnergy Insights program in July 2021 included the SINs (and other personal information) of certain NS Power customers and was among the data that was targeted for exfiltration by the threat actor. Upon discovery by the Company, the Azure storage was immediately locked down.

On June 25, 2025, Nova Scotia Power publicly committed to permanently deleting instances of SINs that remained in the Company's systems. The Company has initiated a process to identify and remove instances of SINs contained within its records. This search has progressed significantly and is being conducted with the assistance of external experts. Except where SINs are legally required for tax reporting purposes, any such information identified will be securely deleted. NS Power anticipates obtaining confirmation of its completion of this process by March 31, 2026.

9.0 CONCLUSION

NS Power trusts that the foregoing addresses the NSEB's direction with respect to the information requested in its letters of July 14, 2025 and November 7, 2025.

NS Power experienced a sophisticated cyberattack discovered on April 25, 2025, with evidence of unauthorized access beginning around March 19, 2025. While customer and Company data was exfiltrated and internal business technology systems were affected, there is no evidence that operational technology or energy delivery systems were accessed or disrupted. NS Power activated incident response and business continuity protocols, engaged Mandiant under counsel, and notified CCCS, RCMP, CSIS, and the FBI; the Company also reported the incident to the Office of the Privacy Commissioner of Canada and continues to cooperate with their investigation.

To protect and inform customers, NS Power issued staged notifications while also advising former customers and expanding the complimentary offer of TransUnion credit and identity monitoring to five years (which includes protective measures such as access to identity restoration services, and up to $1,000,000 of expense reimbursement insurance related to identity theft). The Company has also maintained a multi-channel communications program, established a dedicated call center staffed by TransUnion, and provided in-person community support, guidance, and dark-web monitoring updates as the investigation proceeded.

Recovery and resilience efforts continue, including [redacted] Consistent with commitments made publicly, NS Power is eliminating SINs from systems (except for limited legal requirements) and is working to reconnect customer meters to billing systems; ongoing progress, system restoration timelines, and Board-related matters are tracked in the appended charts and monthly updates.

Finally, NS Power submits that many of the Premier's requests of the NSEB by letter on December 3, 2025 have been already addressed through the various materials provided as part of this proceeding, or will be as part of future proceeding deliverables, including NS Power responses to Board IRs issued on December 3, 2025. Given the relation of the billing concerns to the Incident, it is appropriate to have them considered as part of this process.

Executive Summary

The following page outlines the key initiatives that are currently in flight to support our recovery and restoration efforts. Percentage completion has also been provided to inform our progress on our restoration journey.

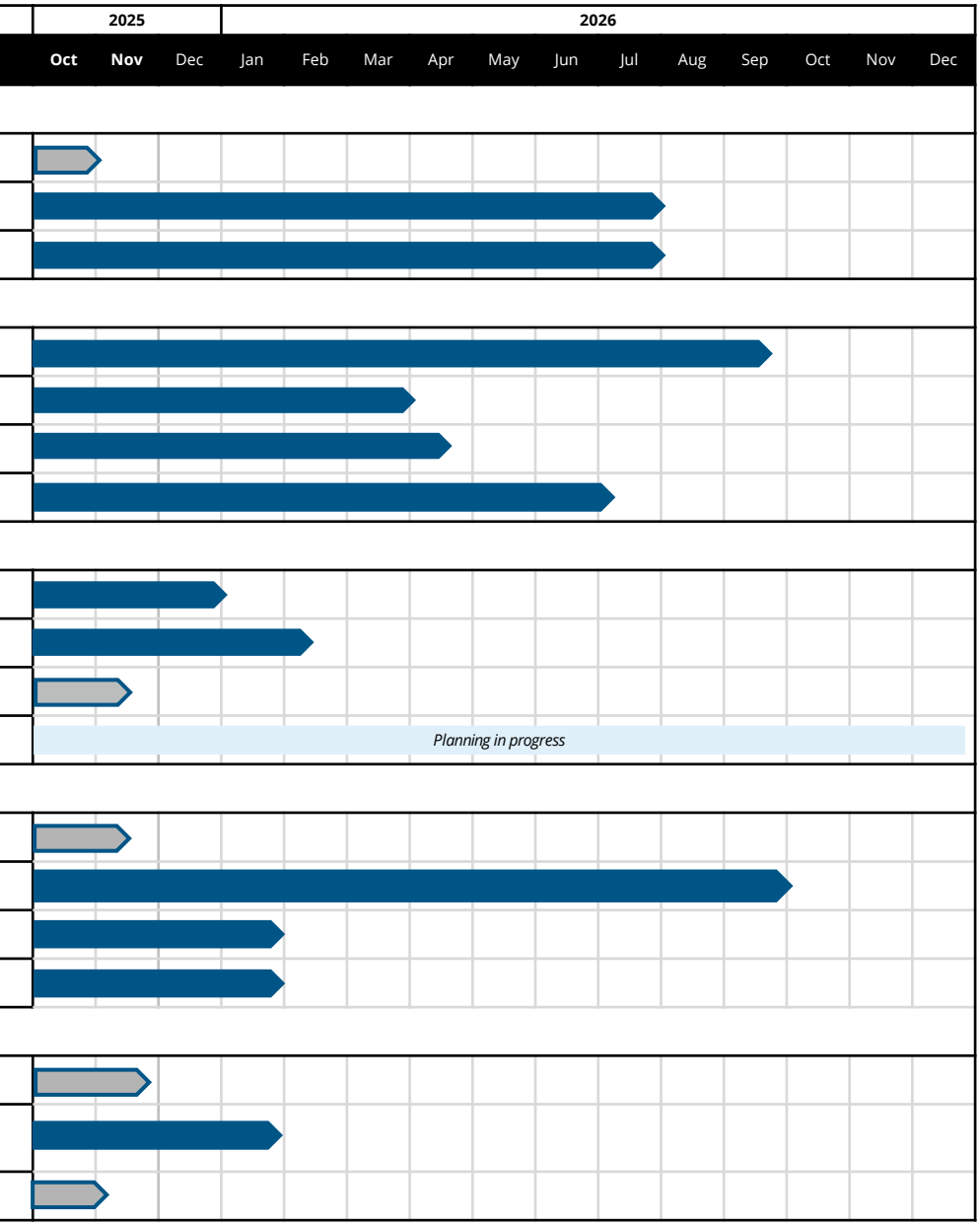
PROGRAM STRUCTURE

The Restoration Program is structured into five (5) key portfolios of work – focusing on restoring business capabilities.

Portfolio	Scope Summary
Enterprise Resource Planning (ERP)	Recovery and restoration of core enterprise resource planning systems—PeopleSoft Payroll, PowerPlan, and Oracle Fusion—to ensure continuity of payroll, financial, and asset management operations.
Customer	Recovery and restoration of advanced metering systems, distribution operations platforms, and customer-facing platforms (such as contact centre and online account services) to ensure accurate billing, service delivery, and accessible customer support.
Additional Capabilities	Recovery and restoration of critical supporting capabilities, including energy trading systems, plant information, engineering document repositories, inventory management, and end-user computing.
Cybersecurity	Restoration of foundational cybersecurity controls and protections to ensure safe, secure and resilient operations.
Technology Enablement	Recovery and restoration of core technology infrastructure – including network, backup and disaster recovery, servers and other data centre equipment to support the reliable operation of business systems.

Restoration Roadmap

Project	Completion Date	%Complete (Dec 16)
ERP		
Payroll	31-Oct-25	N/A
PowerPlan	31-Jul-26	55%
Oracle Fusion	31-Jul-26	25%
CUSTOMER		
MyAccount	25-Sep-26	25%
AMI HES	31-Mar-26	50%
ADMS Resiliency	17-Apr-26	50%
MV90	07-Jul-26	40%
ADDITIONAL CAPABILITIES		
Aligne Fuels/PI	31-Dec-25	90%
Adept Restoration	13-Feb-26	40%
PC Replacement	14-Nov-25	N/A
Self-Serve BI & Analytics	TBD	N/A
CYBERSECURITY		
OT Hardening	10-Nov-25	N/A
IAM	30-Sept-26	25%
MDR	30-Jan-26	80%
Vuln. Mgmt.	30-Jan-26	80%
TECHNOLOGY ENABLEMENT		
Network	28-Nov-25	N/A
Data Centre Computer Hardware	30-Jan-26	37%
Backup	4-Nov-25	N/A



The dates shown in this Gantt chart represent the current planned schedule for the Restoration Program Office (RPO) initiatives. These timelines are subject to change based on evolving priorities, resource availability, and unforeseen dependencies.

Complete

Active

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Rates-Related Matters					
Time Varying Pricing	Introduced	Updated	Updated	**Update**: Systems required for Evaluation are expected to be available by the end of 2025, with the required data for Year 4 (2024/25) Evaluation work to be available early in Q1 2026. Evaluation activities are expected to be underway through Q1 2026 and wrap up in Q2 2026 with the Evaluation Report to be filed as soon as it is completed. In accordance with the Board Order in M12499, the Company filed an update on, and extension request for, filing this Year 4 Evaluation Report on December 17, 2025. Prior to re-instating TVP rates, the full restoration of: AMI meter communications, a meter data management system, My Energy Insights, and TVP specific technology capabilities and integrations are required. These systems, once online, need to achieve a high level of performance in terms of advanced features and performance in order to administer TVP Rates.	Year 4 (2024/25) Evaluation Report expected to be complete for filing in Q2 2026. All Systems required for the administration of TVP Tariffs expected to be restored by the end of Q3 2026.
Time of Use - Real Time Pricing Tariffs	Introduced	NA	NA	**October 1:** "NS Power provides an annual report regarding its Time-of-Use Real Time Pricing (TOU RTP) tariffs to the NSEB. Due to the Incident, NS Power is unable to prepare the 2025 report (using data from August 2024 to July 2025). Relevant data from January 2025 to April 2025 is available; however, 2024 data on participating customer bills, usage and marginal cost is unavailable, and data from May 2025 onward is estimated. NS Power is the process of investigating the recovery of the relevant files. This is not expected to have an impact on customers."	RTP report will be completed in Q2 2026.
Extra Large Industrial Active Demand Control Tariff &One-Part RTP Tariffs	Introduced	Updated	Updated	**December 1:** "Since NS Power's last monthly update, NS Power has re-established the connection between Hitachi's Portfolio Optimizer (PortOps) software and NS Power's network, as well as re-established the Plant Information (PI) data system environment to reconnect to plants and systems and has begun to populate the necessary databases to restore the dependent processes. As noted in the Third Monthly Update Report, these systems are essential for re-establishing processes related to evaluating the ELIADC and determining the cost to serve PHP and One-Part RTP."	Data processing and PortOps modelling for the 2025 period is expected to be completed by January, 31, 2026.
Renewable to Retail Information	Introduced	NA	NA	**October 1:** "NS Power's annual Wholesale and Renewable to Retail Market Report provides Cost of Service by Functional Areas in cents per kWh pursuant to Renewable to Retail market-related historical NSEB direction. This information was last provided to the Board in the 2024 Wholesale and Renewable to Retail Market Report Appendix 2, filed on February 28, 2025. Due to the Incident, the model used to calculate this information is unavailable. NS Power is in the process of recreating the model, which will take some time. Accordingly, there may be a delay in posting the same information for 2025 and providing this in the February 2026 report."	The model will be available in January 2026.

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Customer Billing					
Customer Billing	Introduced	NA	Updated - Pulled up under the Incident Impact and Response section	**December 1:** "As the Board is aware, customer billing has been affected by the Incident. NS Power continues to address customer concerns as they arise and take proactive steps to address customer questions about estimated bills. As discussed in the Second Monthly Update Report, the Company has implemented a manual meter reading process as the Incident disrupted customer billing processes, online self-service functions, and meter data integration. Customer meters have continued to accurately record electricity usage. To date, approximately 75 percent of customers have now had at least one meter reading since the Incident, and the Company will continue to target the remaining 25 percent until communication with customer meters is re-established. As also noted in the Second Monthly Update Report, in acknowledging that customers' billing experience was impacted by the Incident, NS Power has waived all late fees and paused collections and disconnections activity since the Incident for active customers. The Company is on track to reconnect customer meters with the billing systems beginning in December 2025, with all meters expected to be reconnected by the end of March 2026. NS Power acknowledges and understands customer concerns with the estimated billing process. In the interim, the Company has provided flexible options for customers, such as Equal Billing, pay-what-you-can arrangements, and photo meter reads, along with waiving late fees and interest. As some bills in November have caused concerns about overestimates, the Company is increasingly offering the option of a photo reading of customer meters, allowing for a quicker reconciliation of estimated amounts. An online form has been added to our billing website to allow customers to submit a photo reading. For customers who were under-estimated and an actual meter reading results in a large balance, NS Power will work with customers to allow them to pay the balance over an extended period, up to 24 months. When billing resumed in June, NS Power created website content at nspower.ca/billing to outline the billing process and options available for customers, and since then has included three separate bill inserts to communicate information regarding the impacts of the Incident on billing, and the need to estimate bills and adjust them once meters are read either physically or data is able to be retrieved remotely. These bill inserts have also all included notice of and direction to the website content. NS Power will continue to revise this content to reflect the current customer experience. In addition to the foregoing, in a recent bill insert, NS Power also informed customers of the improvements made to the online customer portal (My Account) including new features and information on updated login screens for better security and user experience."	The Company is on track to reconnect customer meters with the billing systems beginning in December 2025, with all meters expected to be reconnected by the end of March 2026.

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Capital and Ace Plan					
CapitalBudgeting/Finance Data	Introduced	NA	Updated	**December 1:** "As noted in the Second Monthly Update Report, capital budgeting and finance data was affected by the Incident, including detailed 2025 ACE Plan budget data by CI being unavailable, resulting in an inability to produce detailed variance analyses. NS Power's capital asset accounting system (PowerPlan) is now operational, and work is underway to repopulate the system with costs incurred through the outage period. While PowerPlan was unavailable, the Capital Planning teams at NS Power utilized detailed spreadsheets in the interim for business continuity, which allowed for the uninterrupted monthly capital filings, the development of the 2026 ACE Plan, and continued financial reporting requirements."	Full PowerPlan restoration is expected in Q2 2026.
CIS Replacement Project	Introduced	NA	NA	**October 1 (abridged)**: "As noted by the NSEB in its letter of September 17, 2025, the CIS replacement capital project has been delayed by the Incident. NS Power said its investigation into the cybersecurity incident "could impact the direction and timeline" of the project. The Company provided an update on the CIS project status in its compliance filing of September 23, 2025 in M11884. In that submission NS Power provided an updated timeline regarding the project, as shown below: ... Please refer to NS Power's compliance filing in M11884 for further information."	As noted in the October monthly update, an application for this project is expected to be submitted to the NSEB in 2026.
NS – NB Reliability Intertie Project	Introduced	NA	NA	**October 1:** "In the NS-NB Reliability Intertie capital project proceeding (M12217), NS Power, on behalf of Wasoqonatl Transmission Incorporated, produced various sensitivity analyses in response to IRs. Midgard, the consultant for Board counsel, commented on this and the cybersecurity implications in its evidence of July 18, 2025: "Due to an ongoing cyber incident affecting portions of NS Power's Information Technology ("IT") systems, WTI regenerated the sensitivity analyses using the same assumptions and modeling approach. While the outputs differ slightly from those originally filed, WTI stated that: "…the results are of a similar magnitude as those shown in Figure 8 [of the Application] but are not the exact same values. The variances in outcomes are to be expected when rerunning the Plexos optimization engine to solve a complex, multivariable, 22-year problem." Despite these differences, WTI emphasized that "the cost variance in each case is <0.5% of the System NPVRR," which it cited as confirming that the Reliability Intertie "enables the lowest cost long-term solution for the NS electricity system" across a range of plausible futures. Midgard does not view the re-run variances as material or indicative of any flaw in the modeling approach. The supporting information was also resubmitted, as the original files were lost or rendered inaccessible because of the cyber incident." Accordingly, there were no material impacts on the project analysis."	The Reliability Tie project has been approved by the NSEB. Modelling of this nature has been transferred to the IESO-NS.
Financial Reporting and Statements					
Financial Reporting and Statements	Introduced	NA	NA	**Update:** Automated financial reporting and statements have been affected by the cybersecurity incident. Similar to the issue noted above under Capital Budgeting/Finance Data, certain financial systems and data are unavailable as a result of the Incident. As noted in NS Power's Q1, Q2 and Q3 Regulated Financial Statement submissions, forecast figures have been used to estimate certain unregulated adjustments required to be made to the legal financial statements in arriving at the Regulated Financial Statements. The amounts being estimated based on forecast are not material and NS Power expects all information to be available to make these adjustments based on actual figures (as per normal course) for the Q4 2025 Regulated Financial Statements. This is not expected to have an impact on customers.	Q1 2026 (for completion of Q4 2025 Regulated Financial Statements).

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Fuel Adjustment Mechanism					
General	NA	Updated	Updated	**December 1:** "As identified in the Second Monthly Update Report, Fuel Adjustment Mechanism (FAM) related matters have been affected by the Incident. The Company has commenced preparations for the 2024/2025 FAM Audit. Significant progress was made in November to recover prerequisite systems and data required for the 2024-2025 FAM Audit. The PortOps dispatch optimization software has been enabled with a cloud installation, which, together with PI system availability, will allow the business to reinstate dispatch optimization and Annually Adjusted Rates (AAR) reconciliation process. Success was also achieved in restoring a portion of historical network drive information. Effort continues to remediate those areas of the network not initially restored. At present, this includes information related to solid fuel commercial activity and portfolio optimization. While typical data sources may not be available for all anticipated Data Requests, the Company will continue to make best efforts to provide the auditor with an alternative data set to validate the prudency of fuel costs management."	Q1 2026
Maritime Link Benefits Report	Introduced	NA	NA	**Update**: The Q3 Maritime Link Benefits Report was filed on November 10, 2025 and the dollar values related to benefits was unavailable, as previously reported. The PI system has now been enabled and the teams are working to rebuild the data in order to calculate the benefits related to the Maritime Link. This will take some time and it is anticipated the data will not be available for the Q4 2025 report (due to be filed in February 2026). Once the data from PI is available, all benefits related to the Maritime Link will be reported in a future report. This is not expected to have an impact on customers.	Q1 2026
FAM Quarterly	Introduced	NA	Updated	**Update:** The Q3 2025 FAM report filed on November 10, 2025 included manually produced Fuel Reports, in keeping with the Q2 2025 report. The Q4 2025 report (due in February 2026) is also anticipated to include manually produced Fuel Reports. The system that electronically produces the Fuel Reports is expected to be back online late Q1 2026, or in Q2 2026. Cause codes related to PHP under the ELIADC have become available and were included in the Q3 2025 report including the period from April 25, 2025. Once all systems are back online, any discrepancies will be trued up in future reports.	Q1/Q2 2026
Dispatch Study Action Plan Quarterly Update	Introduced	NA	Updated	**Update:** "In its Dispatch Study Action Plan Quarterly Update provided to the NSEB dated December 15, 2025, the Company provided progress updates related to the ECC Optimization Tools Project and confirmed the expectation for final implementation is anticipated to be the end of March 2026.	Q1 2026

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Performance Standards					
Performance Standards	Introduced	NA	NA	**October 1:** "NS Power will continue to assess the extent to which the Incident may have an impact on Performance Standards metrics, but can confirm the following metrics have been impacted: • Regular Business Call Answer Rate: NS Power is currently behind YTD target due to the Incident's impact on call volumes. • Percentage of Bills Estimated: Due to the unavailability of AMI data, the Company relied on estimated bills. Notwithstanding these impacts, NS Power has implemented manual meter reading, limiting the number of estimated bills. The following metrics were not impacted: SAIDI, SAIFI, CKAIDI, CKAIFI, ETR Updates, Outage Reports, Percentage of Customers Restored within 48 hours."	The Company is on track to reconnect customer meters with the billing systems beginning in December 2025, with all meters expected to be reconnected by the end of March 2026.
Affiliate Code of Conduct					
Affiliate Code of Conduct	Introduced	NA	NA	**Update**: Billing of employee time continued through the end of the year 2025 based on estimates. In Q1 2026 the employee time-related billing will be trued up based on actuals. This is permitted under the terms of the ACOC. This is not expected to have an impact on customers. Starting in January 2026 it is anticipated that billing for employee time will resume the pre-cybersecurity incident process, namely billing actuals on a one month lag.	Q1 2026
Interconnection processes			NA		
Hosting Capacity Map and Analysis	Introduced	NA		**October 1:** "As noted by the NSEB in its letter of September 17, 2025, the hosting capacity map and analysis has been affected by the cybersecurity incident. 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". The Incident resulted in the unavailability of GIS apps, which is preventing updates to online maps and displays, including the Hosting Capacity Map. However, NS Power is updating data and models offline to ensure accurate information is provided in related preliminary assessments of distribution connection requests."	Dependent on the GIS recovery and integration between GIS and CYME Software. ETA for this is March 2026.
Processing Interconnection Requests	Introduced	NA		**October 1:** "The Incident has affected NS Power's ability to process interconnection requests in accordance with the interconnection processes. Some system study models, relevant data, and reporting templates, for example, are unavailable, affecting the timely processing of some interconnection requests. Additionally, invoicing and refunding processes, where applicable, have been put on hold until required data is made available again. Mitigation measures taken include recovery of some data, standing up interim processes to minimize impact, and recreating work made unavailable due to the Incident. To date, NS Power has maintained its obligations under the SGIP and DGIP with respect to timelines and processing of Interconnection Requests."	Administration of the SGIP/DGIP, as well as any modelling related to the SGIP has been transferred to the IESO-NS. Return to normal processes for modelling related to the DGIP is dependent on access to PI data and GIS. ETA for this is March 2026.

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Demand Side Management					
E1's Residential Behaviour Program	Introduced	NA	NA	**October 1:** "As noted by the NSEB in its letter of September 17, 2025, the ability to provide relevant customer data to EfficiencyOne (E1) has been affected by the cybersecurity incident. Customer consumption data derived from the Company's AMI meters is unavailable, as well as the My Energy Insights (MEI) platform, which collectively provide E1 support for its various programs and analyses. The Company anticipates that work on reestablishing data flows from AMI meters and the MEI will extend into 2026. Regarding other relevant customer information to inform E1's programs, NS Power is considering how best to provide this information in a usable and secure manner. In the meantime, NS Power continues to meet with E1 on a regular basis to discuss the issues regarding the provision of data and possible near-term interim solutions."	The Residential Behaviour program will require a minimum of 1 bill cycle following the reintroduction of data into MEI before it can produce results. Forecast restoration is by end of Q3 2026.
E1's Demand Response Programming	NA	Introduced	NA	**November 3:** "The Company continues to coordinate with E1 on demand response (DR) events, which will proceed independently of the TVP program. NS Power will continue to notify E1 of DR events, and E1 will continue to administer its DR program. AMI data will not be available for evaluation, measurement and verification of the DR programming for the upcoming winter season. E1 has confirmed that device-level data will continue to support performance validation for its residential 'Eco Shift' program, and that alternate approaches (e.g., dataloggers) are being implemented to ensure accurate measurement of commercial 'Smart Synergy' events at the facility level. The Company continues to support E1 in its efforts to maintain program continuity."	Data flows to evaluate Demand Response will be restored in Q3 2026, ahead of the 26/27 Season beginning on Dec 1, 2026, pending successful restoration of AMI and relevant systems.
System Planning					
System Planning	Introduced	NA	NA	**October 1:** "In response to Natural Forces IR-1 (and Energy Storage Canada IR-5) under the 2025 Evergreen IRP Action Plan and Roadmap Update proceeding (M12247), NS Power advised of its inability to access certain historical and simulated data: "The Evergreen IRP Model did not model exports. For the net load reductions from demand-side measures, please refer to the 2023 Load Forecast Report for the DSM values on an annual basis. Due to the cyber incident continuing to affect portions of NS Power's IT system, it is not possible to provide all of the requested hourly data at this time. Our IT team is working diligently with cyber security experts to bring the affected portions of our IT system back online. However, please see Attachment 1 for the requested data for 2024 (for the peak hour) and the requested data for 2030 and 2035 pulled from the NS-NB Reliability Intertie model." Relatedly, as referenced above under NS-NB Reliability Intertie, historical PLEXOS models were unretrievable as a result of the Incident. However, as noted above, NS Power was able to recreate the models on an interim basis allowing the Company to continue with system planning activities, while efforts continue to retrieve the historical models over time. This is not expected to have an impact on customers."	IRP Modelling has transitioned to the IESO-NS

Affected Regulatory Matters	Report 2 - October 1	Report 3 - November 3	Report 4 - December 1	Latest update	Forecast Restoration of Normal Activities
Miscellaneous					
Maritime Link Q2 2025 Quarterly Report	Introduced	NA	Updated	**December 1:** "As noted by the NSEB in its letter of September 17, 2025, the detailed allocation between the Maritime Link Project and sustaining capital costs is unavailable at this time due to the Incident, as reported by Nova Scotia Power Maritime Link (NSPML) in its Q2 2025 report. The NSEB went on to comment that "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". This issue has now been resolved and the allocation of the Maritime Link Project and sustaining capital costs was reported by NSPML in its Quarterly Report filed on October 15, 2025"	As noted: This issue has now been resolved and the allocation of the Maritime Link Project and sustaining capital costs was reported by NSPML in its Quarterly Report filed on October 15, 2025.
Joint Use Agreement Proceeding	Introduced	NA	Updated	**December 1 (abridged)**: "While some of the GIS services have been restored, the integrations required for the Joint Use tracking and reporting remain unavailable. GIS service restoration work continues with the necessary integrations expected to be available in Q1 2026. As noted in NS Power's Rebuttal Evidence and Final Submissions filed on November 17, 2025, although the new processes outlined in the Letter of Intent (LOI) have been in effect since March 3, 2025, the formal agreement referenced in the LOI has not yet been executed. NS Power and Bell have continued to advance discussions and conduct preliminary analysis using available data, and both parties anticipate formalizing the agreement in 2026. The matter is currently open before the NSEB by way of a written hearing proceeding."	Q1 2026
Customer Energy Management (CEM) Evaluation, Measurement, and Verification (EM&V)	Introduced	Updated	NA	**November 3:** "As only AMI data up to March 31, 2025 will be available for analysis for 2025, the My Energy Insights (MEI) platform is unavailable, and associated data, analysis and customer alerts are therefore also unavailable. In the interim, NS Power is consulting with Econoler to develop an alternative 2025 CEM EM&V approach that reflects the data limitations identified in this report, and will provide the proposal to the NSEB for their consideration upon completion."	Q3 2026

M12457 DIRECTION

As noted in the introduction of the main Cyber Incident Report, the NSEB directed NS Power to address the broader review outcomes arising from M12457.

Each of the Board's questions are addressed in turn below.

1. ***Confirming the inability of demand registers to reset remotely at the end of each billing cycle was limited to single-phase meters.***

   The inability of demand registers to reset remotely at the end of each billing cycle is limited to single-phase meters installed at commercial service locations.

2. ***Confirming which rate classes were impacted.***

   The impact is limited to a small subset of customers within the General Demand and Small Industrial rate classes.

3. ***How many demand billing customers were impacted by the inability of demand registers to reset remotely at the end of each billing cycle?***

   There are 1,454 demand billing customers with single-phase meters. After an initial review, NS Power has identified that 1,056 of those customers have been impacted by the inability to remotely reset demand registers on the meters.

4. ***Has every demand billing customer with a single-phase meter been advised of the potential issue with the demand register resets? If so, how was this done? If not, why not?***

   NS Power will be communicating with all customers once our investigation is complete. The investigation process has taken significant effort to confirm the customers potentially impacted by the issue. The initial investigation required the reconciliation of meter installation records, rate classifications of accounts, meter reading records and billing records. NS Power will be communicating to the confirmed impacted customers in early 2026.

5. How many demand billing customers have been contacted about the issue?

NS Power has been in contact with 35 customers impacted by this issue.

6. How many demand billing customers have had their charges investigated?

NS Power has completed an initial investigation of the charges for all 1,454 customers, but this investigation remains ongoing.

7. How many, if any, demand billing customers have yet to have their accounts reviewed? If there are any, when will the process be completed?

An initial review has been completed of all the single-phased demand billing customers impacted by this issue to confirm the scope of impacted customers. This review is currently in progress and will be completed in early 2026.

8. Is there a standardized methodology for determining the impact on demand billing customers, of the inability of demand registers to reset remotely, including a standard rate recalculation methodology? If so, please describe each step, including how many billing cycles are being reviewed for each customer. If not, how is NS Power making sure that all demand billing customers are being treated equally and being billed appropriately?

There is no standardized methodology for determining the impact on single-phase demand billing customers from the inability of demand registers to reset remotely.

NS Power is reviewing all individual bills of the 1,454 customers since the cyber-incident in April and the loss of the remote demand reset functionality. Each bill will be considered against the billing history of the customer for the same month of the previous year, with changes to the year over year usage being factored in. If the actual demand reading used for billing in 2025 is determined to be impacted by the inability to be reset, the demand value from the same bill of the previous year will be taken into consideration in determining any necessary credits.

9. How many refunds or credits have been issued to demand billing customers?

The number of credits issued to customers to date is 35.

10. What is the total dollar amount of all refunds and credits?

The total dollar amount of credits issued to date is $10,497.

11. Have any reviews resulted in increased demand billing charges for customers? If so, how many customers were impacted and what is the total dollar amount of any billing increases?

The initial part of the review process has identified increased demand charges for 1,056 customers. The dollar amounts per customer are currently being verified. This process will be completed in early 2026.

12. How many single-phase meters are currently in service?

Single-phase meters currently service the over 550,000 service locations of all non-demand billing customers. They are also in service at the 1,454 meter locations discussed in this matter.

13. How many single-phase meters has NS Power replaced with polyphase meters for demand billing customers?

Single-phase meters can't be replaced with polyphase meters. The meter type required at a service location is dictated by the service type. Polyphase meters are required for locations serviced with three-phase power.

14. If not all the single-phase demand billing meters have not already been replaced, when will the remaining single-phase meters be replaced? Please provide a schedule for the retirement and replacement of the single-phase demand meters.

As previously noted, single-phase demand meters can't be replaced with polyphase meters. Single-phase meters for demand billing customers will always be required. The meter type required at a service location is dictated by the service type not the

rate class. Polyphase meters can only be installed at service locations requiring three-phase power supply.

An AMI single-phase meter product with a physical external demand reset feature is currently not available to NS Power. Procuring a new meter type with these specifications requires a 6-10-month lead time with the meter vendor. The replacement of the 1,454 current meters would then take another 1-2 months. This option is currently being reviewed.

15. Has NS Power found a long-term solution to this issue through consultation with the meter vendor? If not, please elaborate on any short-term solutions while long-term solutions continue to be investigated.

A long-term solution is to procure a new product from the meter vendor of a single-phase meter with an external demand reset lever. This would be a new version of the current single-phase meter product to NS Power's fleet. The meter vendor has indicated that such a product is currently not available. The lead time on the procurement of a new meter product is estimated at 6-10 months. This option is currently being reviewed.

The best short-term solution is the re-establishment of AMI systems. This enables the remote resetting of demand on single-phase meters. It also enables the on-site resetting of demand at single-phase meters by NS Power field resources using field tools.

Other short-term solutions under consideration include a review of the energy usage history for each of the impacted customer accounts for possible reclassification to the Small General non-demand rate class.

16. Please elaborate on any contingency planning associated with the loss of functionality of AMI meters.

NS Power has activated contingency plans for key functions enabled by AMI.

For remote meter reading enabled by AMI, a contingency plan has been activated for field meter reading, using a combination of internal and contractor resources to manually read meters and send those reads to the NS Power billing systems.

For remote connect / disconnect enabled by AMI, a contingency plan has been activated to have connects and disconnects dispatched as field work orders and performed by field crews.

For remote meter configuration changes enabled by AMI, a contingency plan has been activated to perform meter change-outs when needed to facilitate a customer requirement. This work is typically installing a bi-directional meter for a new solar customer.