Nova Scotia POWER
An Emera Company

PO Box 910 • Halifax, Nova Scotia • Canada • B3J 2W5

October 1, 2025

Crystal Henwood
Clerk of the Board
Nova Scotia Energy Board
1601 Lower Water Street, 3rd Floor
Halifax, NS B3J 3S3

Re: M12273 – Nova Scotia Power's Cybersecurity Incident – Monthly Update 2

Dear Ms. Henwood:

On July 14, 2025, the Nova Scotia Energy Board (NSEB, Board) directed Nova Scotia Power (NS Power, the Company) to file monthly progress reports about its response to the recent cybersecurity incident that impacted NS Power (Incident) and its progress in preparing the requested report about the Incident (Incident Report). The Company's first monthly report was filed on August 20, 2025, in response to the brief direction provided by the Board, which stated:

> Pending the filing of the incident report with the Board, NS Power is directed to file monthly progress reports about its response to the event and its progress in preparing the requested incident report. [1]

Preparation of the requested Incident Report remains on schedule to provide to the Board on or before December 31, 2025.

In its correspondence of September 17, 2025, the Board provided further expanded direction on what is to be included in subsequent monthly reports. In accordance with the NSEB's expanded direction, this monthly update provides details regarding the Recovery Program Office (RPO), incident impact and response, ongoing regulatory matters, and timelines. Each is described in the sections that follow below.

The information provided in this report is complete as at the time of filing to the best of NS Power's knowledge. As new information becomes available regarding any of the foregoing, and additional progress is made in the Company's recovery efforts, it will be reflected in these monthly update reports.

[1] NSEB Letter re: M12273 – Board Inquiry into Nova Scotia Power's Cybersecurity Incident, July 14, 2025, p.3.

Incident Impact and Response

NS Power's ability to deliver power to customers — its primary mandate — was not affected by the Incident. Where there were customer impacts from an operational or service perspective, these were related to changes in how customers engaged with the Company. The most significant impacts of the Incident affected internal business operations; the Company and its employees rapidly pivoted to alternate processes to sustain business operations.

The initial focus was on containment and incident response. Once the IT environment was secured, NS Power shifted to executing business continuity processes, including manual meter reads, estimated billing, and manual financial processes. As these measures stabilized operations, focus transitioned to the structured recovery and restoration program now managed through the RPO.

The incident affected multiple areas of the business operations in different ways. The following outlines the functional impacts experienced, the steps taken to maintain continuity, and the progress achieved to date in restoring these business capabilities.

Cybersecurity

The operation of cybersecurity capabilities is a critical aspect of recovery, ensuring that business services are restored in a secure and controlled manner. As technology services are reintroduced, the cybersecurity team validates that appropriate controls are in place and operating effectively. Please see NS Power's response to NSEB IR-01(a) (M12273) for additional information.

Financial Enterprise Resource Planning

The Incident disrupted the Company's Enterprise Resource Planning (ERP) systems. The ERP systems are comprised of core financial management functions, including general ledger, capital accounting, and payroll operations.

In the immediate aftermath of the Incident, manual processes were established to sustain statutory reporting and to enable estimated payroll calculations. These interim measures allowed continuity of financial oversight while reducing risk to customers, employees and the business.

Since then, payroll operations have been fully stabilized, and normal pay cycles have resumed. Interim solutions remain in place for capital accounting and reporting while the broader financial management environment is being restored. The Company is returning to normal invoice payment volumes as its business continuity processes mature and system

restoration progresses. Core finance functionality is scheduled to come back online in time to support statutory reporting obligations later this year.

Customer Billing and Customer Systems

While meters have continued to accurately record electricity usage, the Incident disrupted customer billing processes, online self-service functions, and meter data integration. In the immediate response, customers were supported through estimated billing supplemented by manual meter readings, while engagement was redirected to call centre channels where online options were limited. These measures safeguarded continuity of service despite the change in customer experience.

Recovery efforts have since stabilized core customer engagement channels, and contact centre operations are now fully functional. Online account access and billing capabilities have been restored, while work has commenced to reinstate automated meter data integration. NS Power expects customer billing and engagement processes to return to business as usual in early 2026, with interim measures maintained until that time to ensure continuity for customers.

Technology Enablement

The Incident disrupted foundational technology services, which created dependencies that impacted the restoration of some business functions and required employees to rely on contingency solutions.

To address these challenges, a secure network rebuild has been initiated, and corporate computer devices have been re-imaged or refreshed as needed to strengthen security and ensure continuity of operations. A dedicated program has also been launched to re-establish robust backup capabilities. Efforts are also focused on re-enabling data flows and system integrations to support the recovery of business applications. These foundational services are progressing steadily and remain a central focus of the restoration program.

Additional Capabilities

The Incident affected several enabling business systems, including energy trading platforms, performance and fuel data, asset management, and regulatory reporting tools. This required business units to adopt manual processes and alternate reporting approaches to maintain continuity of operations and regulatory compliance.

Core trading functions have now been stabilized and restored to operational use. Work continues to re-establish performance and fuel data systems, alongside projects to reintroduce asset management, energy management, and document integrity functions.

NS Power anticipates some restoration activities being complete in Q4 2025, with some carrying forward into 2026 and beyond. Mandatory regulatory reporting remains ongoing, supported by interim processes where required.

Recovery Program Office

The RPO has continued to advance recovery activities across all major business and technology areas. The RPO was established following the incident response to coordinate recovery and restoration efforts across the enterprise. The RPO functions as the central program management office, ensuring structured governance, risk management, and progress reporting. The RPO includes representation and input from various business units, consisting of approximately 30 personnel between employees and consultants.

The RPO is focused on the following areas:

- Program Delivery Governance – Integrated program planning, scheduling, and risk/issue management.
- Regulatory and Insurance Advisory – Oversight to support regulatory and insurance obligations.
- Resourcing – Workforce and resource considerations, including capacity planning.
- Internal Controls – Embedding financial and operational control requirements in recovery activities to support SOx and National Instrument 52-109 (Certification of Disclosure in Issuers' Annual and Interim Filings) requirements.
- Security Control Office (SCO) – Defining and monitoring cybersecurity requirements across in-flight projects.
- Enterprise Architecture – Ensuring technical design aligns with long-term business and security needs.
- Organizational Change Management (OCM) – Supporting employees and business units in adapting to new systems, processes, and ways of working.
- Reporting and Communications – Delivering consistent reporting on program health to management, employees and customers.
- Privacy and Data Management – Ensuring that enhanced data security measures such as additional access controls and end-point protections have been implemented.

The RPO is staffed by senior leaders and dedicated program management resources, supported by external advisors where needed.

Ongoing Regulatory Matters

As a result of the impacts noted above, several matters before the Board have been affected, including:

- rates-related,

- customer billing,
- capital and ACE Plan,
- financial reporting and statements,
- Fuel Adjustment Mechanism,
- reliability and performance standards,
- Affiliate Code of Conduct,
- interconnection processes,
- demand side management,
- system planning, and
- other miscellaneous matters

The response and restoration arising from the Incident is dynamic, and consequently timelines and impacts may evolve as restoration progresses. As impacts to regulatory filings are identified they are then communicated to the Board and stakeholders in a timely and transparent manner. This approach ensures that all parties involved in the specific matters are directly communicated with regarding how the matter may be impacted. As the Board has now requested, the identified impacts as understood to date are included in the sections that follow.

Rates-Related Matters

Rates-related matters have been affected by the Incident.

Time Varying Pricing

As noted by the NSEB in its letter of September 17, 2025, the Time Varying Pricing (TVP) matter has been affected by the Incident. NS Power will be filing a letter with the Board with its proposed approach for the upcoming TVP season.

Time of Use-Real Time Pricing Tariffs

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.

Extra Large Industrial Active Demand Control Tariff and One-Part RTP Tariffs

The Extra Large Industrial Active Demand Control (ELIADC) Tariff provides, in part, the following:

Annually, NS Power shall report to the Board to confirm the dollar value of

> system savings that have been achieved through Active Demand Control of PHP's load under the Protocol, taking account of the impacts of any variances by PHP from the dispatch schedules issued to it by NS Power and any adjustments arising from schedule variances if required. NS Power shall endeavor to submit this report no later than 60 days after the end of a tariff year.
>
> PHP will be entitled to a credit equal to 25 percent of the cost differential between the CBL Energy Charge and the actual annual cost to serve PHP during the given tariff year. Such payments to the Customer will be made via an annual lump sum payment.[2]

As a result of the Incident, NS Power's systems required to calculate the cost to serve under the ELIADC and for calculating the dollar value of system savings achieved through Active Demand Control (ADC) of PHP's load are not currently available. The cyber incident also impacted systems required to calculate the accounting cost of solid fuel which would be attributed to PHP. These systems are also required for the calculation of PHP's CBL cost for 2026. Of note, NS Power is working to file a new tariff attributable to PHP by the end of 2025, which will be effective at some point in 2026, pending NSEB approval.

In addition to impacting the cost to serve calculations for the ELIADC, these systems are required for the calculation of the cost to serve for the One-Part RTP Tariffs.

Once these systems are restored, NS Power plans to run calculations for each month in which the data was unavailable to establish the above-described ADC evaluations and the cost to serve under the ELIADC and One-Part RTP Tariffs.

Renewable to Retail Information

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.

Customer Billing

As the Board is aware, customer billing has been affected by the Incident. NS Power continues to address any customer concerns as they may arise, but as discussed in the foregoing, the Company has implemented a manual meter reading process, significantly

[2] Extra Large Industrial Active Demand Control Tariff

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

Capital and ACE Plan

Capital Budgeting/Finance Data

In general, capital budgeting and finance data has been affected by the Incident. For example, detailed 2025 ACE Plan budget data by CI is unavailable, resulting in an inability to produce detailed variance analyses. Moreover, as NS Power's capital asset accounting systems are currently offline, actual capital project spend is temporarily unable to be verified. NS Power noted this issue in its Tusket Q2 2025 Contingency Report (M10197) filed with the NSEB on July 25, 2025 where it stated "Spend-to-Date values are prepared using a combination of Q1 2025 spend-to-date values and forecast due to limitations of business applications as a result of the cybersecurity incident and associated incident response. Actual Q2 2025 spend-to-date values are not expected to change materially from forecast and any adjustments will be reflected in the Q3 report."[3] The Company advised of the same in its Annapolis bi-annual report (M10013) filed with the NSEB on July 25, 2025.

To mitigate the effects of the temporary unavailability of these systems and associated data, the Capital Planning teams at NS Power have created detailed spreadsheets in the interim for business continuity, which auto-calculate certain capital financial metrics which are then reviewed in detail by the Finance teams for reasonableness. This process is being utilized for the development of the 2026 ACE Plan and associated capital projects.

This is not expected to have an impact on customers.

CIS Replacement Project

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:

[3] NS Power Letter re: M10197 – CI 29807 - HYD – Tusket Main Dam Refurbishment – Application (ATO) – Project Update – Q2 2025 Contingency Report (Contingency Report 25), July 25, 2025, Appendix A, p.2.

Previous Expected Timeline	Activity	Current Expected Timeline
Q4 2023 - Q2 2024	Identify requirements for and completion of competitive solicitation for Planning and Procurement partner.	Complete
Q3 2024 - Q1 2025	Develop plan for CIS Replacement Procurement (RFP).	Complete
March 25, 2025	Issue RFP for CIS Replacement Solution and System Integrator Services.	Complete
Q2 2025	Evaluate Proposals and Recommendation for CIS Replacement Solution and System Integrator (Project paused during this stage).	2026
Q3 2025	Develop Capital Filing	2026
Q3 2025	Application to NSEB	2026
Q1 2026	NSEB Decision	2027
Q2 2026	Start CIS Replacement Project	2027
Q2 2028	Launch new CIS System	2029

Please refer to NS Power's compliance filing in M11884 for further information.

NS-NB Reliability Intertie

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.[4]

Accordingly, there were no material impacts on the project analysis.

Financial Reporting and Statements

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 and Q2 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) by the end of 2025.

This is not expected to have an impact on customers.

Fuel Adjustment Mechanism

Fuel Adjustment Mechanism (FAM) related matters have been affected by the Incident.

Maritime Link Benefits Report

In the Q2 Maritime Link Benefits Report submitted to the NSEB on August 18, 2025, the Company provided the following:

> Apart from the dollar values, which NS Power is unable to compile until the data presently unavailable due to the cyber incident is recovered, this report contains the items directed by the Board applicable to NS Power.[5]

This data is expected to be unavailable for the Q3 report.

This is not expected to have an impact on customers.

FAM Quarterly Reports

[4] Midgard Submission, Re: Review of Wasoqonatl Transmission Incorporated – NS-NB Reliability Intertie Project Application (M12217), July 18, 2025, p.52.
[5] NS Power 2025 Q2 Maritime Link Benefits Report, August 18, 2025, p.4.

In the Q2 FAM report covering letter of August 18, 2025, the Company provided the following:

> The Fuel Reports that are submitted as part of the Quarterly FAM report in tabs 1-30 are derived from an enterprise resource system which NS Power cannot access. As a result, these reports have been manually produced for Q2 2025. Upon restoration of the system, NS Power will reconcile the reports submitted as part of the Q2 2025 FAM report to the reports produced from the enterprise resource system. NS Power will incorporate any prior period adjustments required as part of future FAM reporting.[6]

Additionally, Cause Codes related to PHP under the ELIADC have not been available for reporting. This was conveyed in the Q2 FAM report filed on August 18, 2025, tab Q13 footnote 2. An update to this was provided during the FAM SWG meeting on September 26, 2025, stating:

> The cause codes during the period were impacted by the cybersecurity event. From April 25 to August 5 ECC dispatched load in real time, without NSP Marketing providing PHP with a real-time dispatch schedule. When PHP was unable to comply with ECC dispatch instructions, the reason was documented. There were three hours in the quarter when PHP was unable to follow dispatch per ECC instruction (Cause Code 5). Code tracking related to failure to load due to equipment or process constraints, (Cause Code 3), were also tracked and were the lowest in the past 5 quarters at 127 recorded instances. Because there was no marketing dispatch schedule provided to PHP, and only ECC's real time instructions, Cause Codes: 1 – ECC ramp up, 2 – ECC ramp down and 4 – Mutual agreement, cannot be applied. NSP Marketing providing PHP with real-time dispatch schedule resumed on August 5th. [7]

However, the majority of the data for the FAM report was able to be created through different processes, with a high degree of confidence that the data is accurate. Once systems are back online, any discrepancies will be trued up. This data is expected to be unavailable for the Q3 report.

This is not expected to have an impact on customers.

Dispatch Study Action Plan Quarterly Update

As noted by the NSEB in its letter of September 17, 2025, the Company advised in its Dispatch Study Action Plan Quarterly Update dated June 30, 2025 that the Incident impacted the project's expected progress and implementation date and that the ECC Optimization Tools project schedule recovery plan and new implementation dates remain to be determined.

[6] NS Power Letter, Re: Q2 2025 FAM Report, August 18, 2025, p.2.
[7] FAM SWG Presentation, September 26, 2025.

The ECC Optimization Tools Project, which addresses the items in the Dispatch Study Action Plan, has been impacted by the Incident in two key areas. One related to vendor solution access which was disconnected by the vendor as a precautionary measure; the second was due to integration dependencies on some of the core technology solutions within the NS Power IT infrastructure that were impacted by the Incident.

The Project team engaged with representatives of the Recovery Program Office and Cyber Security teams to work on prioritization of specific components to aide in replanning of this project. The team also worked with the vendor to provide necessary risk assurances in order to re-connect to their solution and to continue development and testing.

This effort has resulted in the establishment of a revised implementation schedule to the end of March 2026. This revised schedule is subject to potential change dependent on actual vendor reconnection dates and progress in restoring the core technology solutions within the NS Power IT infrastructure. During the Q2 FAM SWG meeting held on June 27, 2025, stakeholders were advised that the timeline would be impacted, and greater clarity on timing was provided during the Q3 FAM SWG meeting held on September 26, 2025 to reflect an anticipated go-live date of March 2026.

This is not expected to have an impact on customers.

Performance Standards

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.

Affiliate Code of Conduct

Affiliate Code of Conduct (ACOC) processes have been affected by the cybersecurity incident.

Billing NS Power employee time to affiliates has been based on estimates due to the Incident. However, NS Power employees continue to track their time, which will be billed and a true up will occur to reconcile estimates with the actual costs. This is permitted under the terms of the ACOC. All employees continue to be required to complete the annual ACOC training to ensure employees understand their obligation to protect NS Power confidential information.

This is not expected to have an impact on customers.

Interconnection Processes

Interconnection Processes related matters have been affected by the Incident.

Hosting Capacity Map and Analysis

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.

Processing Interconnection Requests

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.

Demand Side Management

E1's Residential Behaviour Program

As noted by the NSEB in its letter of September 17, 2025, the ability to provide relevant customer data to Efficiency One (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.

System Planning

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.[8]

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.

Miscellaneous

Nova Scotia Power Maritime Link Q2 2025 Quarterly Report

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".[9]

The NS Power internal systems affected by the cybersecurity incident that in turn affected NSPML's ability to provide a detailed allocation between the ML project and sustaining capital costs include the capital asset accounting applications as noted above under *Capital Budgeting/Finance Data*. Restoration efforts are ongoing as noted above under *Incident Impact and Response*.

In the meantime, NSPML advised in response to NSEB IR-1 regarding the NSPML 2026 Assessment Application (M12394) efforts and the effect of the cybersecurity incident:

> a) The cybersecurity incident experienced in the Spring of 2025 by NS Power did not affect the operations of NSPML's assets. However, with

[8] Natural Forces IR-1, NS Power 2025 Evergreen IRP Update (M12247), July 15, 2025.
[9] NSEB Letter M12273 - Board Inquiry into NS Power Inc.'s Cybersecurity Incident - Monthly Update #1 and Confidentiality, September 17, 2025, p.4.

> respect to information technology, much of NSPML's data was not accessible for a period. Some data has since been made accessible and NSPML continues to work with the corporate Emera team to complete accessibility efforts.
>
> b) There are no proposed NSPML O&M costs for 2026 related to or affected by this cyber incident.[10]

This is not expected to have an impact on customers.

Joint-Use Agreement Proceeding

The Joint-Use Agreement Proceeding (M12149) has been affected by the cybersecurity incident.

NS Power's response to NSEB IR-2 part (b), submitted to the Board on June 16, 2025, provided the following:

> The costs to install new poles or replace existing ones are capital costs. NS Power has not completed an analysis of annual OM&G costs for poles covered by the JUA compared to the same OM&G costs assuming NS Power had to own and maintain all the required poles without any cost sharing with Bell Aliant. Due to the cyber incident, an analysis cannot be completed at this time.[11]

NS Power's response to CA IR-3 parts (b), (d) and (e), submitted to the Board on August 20, 2025, provided the following, respectively:

> Prior to the cyber incident, NS Power maintained live data tracking the duration of customer installations. The previous process for Bell Aliant Work Requests often included multiple steps that contributed to delays, such as a secondary site visit by a Bell representative to confirm site requirements, separate payments to Bell and NS Power, and delays in communication from Bell contractors to NS Power to resume installation work. Unfortunately, due to the cyber incident, NS Power is currently unable to access this historical data, as the application used for tracking is unavailable. Greater clarity on the availability of this data may be possible by the fall.
>
> //
>
> Since the cyber incident, NS Power has not been able to formally create new tracking data for service times for power connections as effectively as before, as the links between applications used to track this information are currently unavailable.
>
> //

[10] NSEB IR-1, NSPML 2026 Assessment Application (M12394), September 16, 2025.
[11] NESB IR-2, Joint-Use Agreement Proceeding (M12149), June 16, 2025.

> As noted in responses to part (b) and (d), NS Power had the capability to track installation timelines more effectively prior to the cyber incident. However, the incident has temporarily impacted the Company's ability to access and generate new tracking data for service times related to both NS Power and Bell poles, as the links between applications used for tracking are currently unavailable.[12]

NS Power's response to SBA IR-1 parts (b) and (c) provided the following, respectively:

> Since the signing of the LOI, approximately 175 work orders have been created under the new line extension process. Please note this is an estimated figure, as NS Power is currently unable to validate the actual number of poles installed due to the recent cyber incident, which has limited NS Power's access to the relevant data.
>
> //
>
> The first quarterly Point of Construction Settlement has not yet been completed, as the necessary systems are currently being rebuilt following the cyber incident.[13]

Finally, NS Power's response to SBA IR-2 part (a) provided the following:

> Due to the recent cyber incident, the pole settlement process has been delayed. One of the key systems required for this process, NS Power's GIS, is currently unavailable. GIS serves as the system of record for pole ownership and is essential for identifying the location of poles placed in Bell-owned poling areas. It will also be used to update ownership records once the quantity of poles to be purchased by Bell is confirmed. Without access to GIS, NS Power has not been able to fully execute or review the new process, and therefore, a formal agreement with Bell has not yet been finalized or signed.[14]

While some of the GIS services have been restored, the integrations required for the Joint Use tracking and reporting remain unavailable. NS Power has no further updates on the JUA progress at this time, but notes that the matter is currently open before the NSEB by way of a written hearing proceeding.

Customer Energy Management Evaluation, Measurement, and Verification

The Customer Energy Management (CEM) Evaluation, Measurement, and Verification (EM&V) has been affected by the cybersecurity incident.

[12] CA IR-3, Joint-Use Agreement Proceeding (M12149), June 16, 2025.
[13] SBA IR-1, Joint-Use Agreement Proceeding (M12149), June 16, 2025.
[14] SBA IR-2, Joint-Use Agreement Proceeding (M12149), June 16, 2025.

NS Power files its annual CEM EM&V report in May, which provides an evaluation of the CEM platform on various metrics from the prior year. The 2024 CEM EM&V report, submitted May 1, 2025, was unaffected by the Incident.

However, due to the Incident, 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.

NS Power is actively working to restore AMI data accessibility as previously noted, to ensure a robust, high-quality analysis moving forward.

Recovery Timeline

Initial efforts have focused on restoring the most critical business functions, including customer billing and engagement systems, capital planning and financial processes, payroll, storm response readiness, and energy trading capabilities. These functions have been stabilized or are progressing through restoration in line with the integrated program plan.

The next wave of effort is centered on business enablement capabilities such as enterprise reporting, data integration, and other supporting systems. While significant progress has been made, certain technology components remain under assessment; the RPO will provide updated delivery windows as solution designs and dependencies are confirmed through the integrated planning process.

Full restoration for major capabilities is expected to progress through 2026. Throughout, business continuity measures remain in place to mitigate impacts to customers, employees, and regulatory obligations. The RPO continues to support the prioritization of program efforts in alignment with the expectations of leadership and external stakeholders.

Update on OPC Investigation

As noted in previous reports, 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 is committed to addressing the OPC's concerns and resolving the investigation in an efficient and expeditious manner.

Yours truly,

Judith Ferguson
Executive Vice President, Regulatory, Legal, and Government Relations