Nova Scotia Energy Board

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

M12743

CI C0068714 - IT - Identity & Access Management

NS Power
Rebuttal Evidence

July 7, 2026

NON-CONFIDENTIAL

TABLE OF CONTENTS

1.0 INTRODUCTION

Nova Scotia Power Incorporated (NS Power, Company) filed its capital work order for CI C0068714 – IT – Identity & Access Management (IAM) with the Nova Scotia Energy Board (NSEB, Board) on March 13, 2026.

This project will design, deploy, and configure a modern Privileged Access Management (PAM) ecosystem through the implementation of CyberArk infrastructure and SaaS capabilities, including Endpoint Privileged Management (EPM). In parallel, the project will strengthen the organization's identity governance posture by implementing an enterprise-grade Identity Governance and Administration (IGA) framework. Overall, this initiative will modernize the Company's IAM and PAM environments, reduce cybersecurity risk exposure, enhance regulatory compliance, and create a scalable foundation for future identity-centric security programs.

The Board initiated a written hearing proceeding on April 13, 2026 and established a timeline for the proceeding. NS Power responded to information requests (IRs) from Board staff,[1] the Consumer Advocate (CA),[2] the Industrial Group (IG),[3] the Nova Scotia Department of Energy (NSDoE),[4] and the Small Business Advocate (SBA)[5] on June 2, 2026. Submissions from the CA (CA Submissions) and the SBA (SBA Submissions) were received on June 16, 2026. No other party to this proceeding filed submissions.

The following is submitted as NS Power's Rebuttal Evidence in this matter, addressing the conclusions and recommendations provided by the intervenors.

[1] Exhibit N-5, NS Power (NSEB) RIRs 1-22.
[2] Exhibit N-7, NS Power (CA) RIRs 1-7.
[3] Exhibit N-4, NS Power (IG) RIRs 1-4.
[4] Exhibit N-3, NS Power (NSDOE) RIRs 1-14.
[5] Exhibit N-6, NS Power (SBA) RIRs 1-5.

2.0 RESPONSE TO CA SUBMISSIONS

The CA's submissions raise three concerns and two recommendations, including:

- the prudency of replacing NS Power's prior PAM solutions with a SaaS-based alternative given NS Power's earlier position that the use of cloud environments for NERC-sensitive data was not permissible;
- the amortization accounting implications of replacing existing PAM solutions prior to being fully depreciated;
- concerns regarding NS Power's cost minimization efforts pertaining to sustaining operating costs;
- a recommendation to disallow AFUDC due to project schedule delays attributed to the cybersecurity incident; and
- a recommendation to amend NS Power's request for contingency.

NS Power addresses each of these matters below. The Company does not agree with the CA's recommendations to disallow AFUDC or amend the requested contingency.

2.1 PAM Asset Replacement and Accounting Treatment

The CA expresses concern that NS Power approved an on-premises PAM solution in 2021 (CI 49094), only to replace it with a SaaS-based solution two to three years after the assets were placed in service. The CA questions whether the original PAM project was "reasonably undertaken," given that SaaS solutions were available at the time, and raises concerns regarding the treatment of unamortized asset balances. NS Power addresses these concerns in Sections 2.1.1 through 2.1.3.

2.1.1 NERC-Sensitive Data in the Cloud

The CA references prior IR responses in which NS Power had indicated that a SaaS model did not meet business requirements, as one of the requirements for the original PAM project was that

NERC data could not be stored in the cloud.

That same requirement continues to apply and is satisfied by the current initiative. NERC-regulated data is not included in the project scope and will not be stored or processed within the SaaS environment.

2.1.2 Transition from On-Premises to SaaS-Based PAM

The CA observes that NS Power's 2021 application did not characterize the on-premises solution as temporary but rather "appears to represent the choice to use a 'hybrid' approach as a decision that was made early in the project alternative review process."[6] This observation is accurate. At the time, the hybrid model combining on-premises and SaaS components was selected as best meeting business requirements and reflected the prevailing industry standard for a multi-year deployment involving significant capital investment and operational integration. Since 2021, however, the technology landscape has evolved significantly, with cloud-delivered security platforms becoming the industry norm due to their scalability, reduced operational complexity, continuous vendor-managed updates, and enhanced cybersecurity capabilities.

In addition, IAM technologies are subject to relatively short lifecycles, typically requiring re-investment within a three to five year period to remain effective in response to evolving threats, technologies, and business needs. NS Power must ensure controls remain effective and continue to scale with the organization. Over this period, vendor product roadmaps have also shifted toward a SaaS-first model, particularly for Endpoint Privilege Management (EPM). Consistent with this shift, the on-premises PAM solution exited vendor support in 2025 and reaches end of life in 2026, and therefore no longer receives functional updates.

In this context, NS Power's transition to a SaaS-based solution in 2026 reflects the expected lifecycle progression of critical cybersecurity infrastructure. The on-premises solution fulfilled its

[6] CA Submissions, page 4.

intended purpose over an appropriate period, and the current project represents a prudent modernization aligned with prevailing industry standards and evolving operational requirements. Accordingly, the assets under CIs 49094 and C0054455 will be replaced by the assets under CI C0068714 as NS Power transitions from an on-premises solution to a SaaS-based model.[7]

2.1.3 Amortization Accounting

The CA also raises concerns regarding NS Power's accounting treatment of assets associated with prior PAM projects being replaced by the current IAM initiative. Specifically, the CA submits that NS Power did not identify assets as redundant or decommissioned, nor address the treatment of any unamortized balances. The CA further asserts that, to the extent certain assets may no longer be used and useful, continued depreciation would be inconsistent with Accounting Policy 6350, which requires assets to be written off in the year they cease to be used and useful. [8]

This project represents one of the first applications of amortization accounting approved by the NSEB as part of the 2026–2027 General Rate Application (GRA).[9] Under this approach, an asset's cost is recovered over a fixed amortization period aligned with its expected service life. Once fully amortized, the asset is retired and removed from the books, regardless of whether it continues to provide service. This differs from traditional pooled depreciation accounting, under which assets continue to depreciate until they are physically retired and no longer used and useful.

Consistent with the approved framework, the assets associated with CIs 49094 and C0054455 will not be retired for accounting purposes at this time. Instead, they will continue to depreciate over their approved amortization periods. Upon full amortization, the assets will be retired from service in accordance with Accounting Policy 6420. As these assets will be fully depreciated at the end of the amortization period, no unrecovered net book value will remain on NS Power's financial

[7] Exhibit N-7, NS Power (CA) RIR-1, Exhibit N-3, NS Power (NSDOE) RIR-9.
[8] CA Submissions, page 4.
[9] M12451, NS Power General Rate Application (GRA), Board Decision, March 25, 2026, page 134.

statements. In these circumstances, Accounting Policy 6350 is not engaged, as the approved amortization framework provides for full cost recovery over the prescribed service lives.

There is no duplication of recovery, as the current application seeks approval for new IAM project assets, while the prior PAM assets continue to be recovered under their established depreciation schedules, consistent with the Board-approved methodology.

2.2 Impact of Cybersecurity Incident on Project AFUDC Costs

The CA raises further concerns regarding the AFUDC included in NS Power's application and recommends that the Board disallow a portion of these costs. This position is based on the view that what appears to be a cumulative delay of at least 12 months was primarily caused by "insufficient internal resources," potentially linked to the cybersecurity incident. Specifically, the CA suggests disallowing the monthly and compounding accumulation of AFUDC from April 2025 through March 2026 for the IAM project. [10]

NS Power does not agree with this recommendation.

As stated in NS Power's IR responses, the cybersecurity incident resulted in changes to the project schedule but did not cause an increase in project costs. The variance from the 2026 ACE Plan subsequent submittal estimate is attributable to continued project development, the evolution of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and advancements in available technology since the 2025 estimate was prepared. These changes required more consulting and labour than originally expected. The additional work included splitting originally combined deliverables into separate releases and undertaking further design, validation, and implementation activities to meet the updated CSF and respond to evolving security risks. [11] These cost drivers were independent of any schedule impacts.

[10] CA Submissions, page 5.
[11] Exhibit N-7, NS Power (CA) RIR-4.

While there was a brief pause in project activity between April and May 2025, the project did not remain at a standstill for an extended period. Work resumed promptly, with execution milestones continuing shortly thereafter. The Statement of Work (SOW) for the PAM phase was finalized and executed in June 2025, followed immediately by planning, sequencing, and prioritization activities to support accelerated delivery.

PAM was appropriately prioritized as the initial phase of the program, given its critical role in securing highly privileged accounts. Implementation activities started with CyberArk to establish foundational controls and core PAM capabilities; specifically, the security of personal privileged accounts was delivered in February 2026. Enhancements have continued throughout 2026, including the rollout of Secure Infrastructure Access (SIA), session recording, and expanded cloud security controls.

The CA also suggests that the SIA delay may have been caused by insufficient resources, while acknowledging "this is not known."[12] The adjustment to SIA timing was primarily driven by evolving security requirements and the evolution of the NIST CSF. Implementing SIA within a separate service management network introduced additional complexity, requiring further design and testing to ensure that security controls were strengthened rather than weakened. The resulting change in sequencing was intentional and undertaken to reduce operational and cybersecurity risks associated with secure partner access.

AFUDC associated with the project totaled $85,258 for the period from April 2025 to May 2026, of which only $3,804 accrued during the limited slowdown between May and June 2025, demonstrating that any disruption was temporary and that project execution largely continued. Further, Accounting Policy 6240 (Allowance for Funds Used During Construction) provides that AFUDC does not accrue where a project is delayed for more than one year. As the interruption in this case was brief and did not constitute a prolonged delay, the criteria for suspension of AFUDC

[12] CA Submissions, page 5.

are not met. [13] As such, NS Power submits that the project cost variance is not attributable to the cybersecurity incident and that there is no basis to disallow AFUDC.

2.3 Contingency Budget

The CA submits that the 15% contingency applied to this project is unreasonable given the project's maturity and level of spending, noting that approximately 45% of the budget has been expended and that roughly 80% of AACE Class 3 deliverables have been achieved.[14] On this basis, the CA recommends that the Board obtain an updated actual spend and decision gate assessment, and then consider either reducing the contingency to 10% of the total budget or applying the 15% contingency only to the unspent balance.[15]

As of May 31, 2026, actual spend is approximately $3.96 million and the project has advanced to Decision Gate 6 (DG6), which is the execution phase.

As described in NS Power's application, the risks intended to be covered by contingency include additional work and findings as the project progresses, as well as the incremental resource effort required to address them, particularly in the IGA phase. These risks include potential cost increases from new or modified infrastructure requirements identified during implementation, expanded testing and validation, and additional change enablement efforts to support user adoption. Because NS Power's infrastructure is managed through its managed service provider, OnX, any additional infrastructure work would be performed through that arrangement and treated as consulting costs. Accordingly, contingency was applied only to labour, consulting, meals, and travel within the detailed cost estimate.

The CA's analysis does not fully account for the nature of the remaining work. The IGA deployment, forecast to complete in October 2026, is the most complex and variable component of the project, involving enterprise-wide application onboarding, identity governance framework

[13] NS Power Accounting Policy 6240 – Allowance for Funds Used During Construction, Paragraph 04(b).
[14] CA Submissions, page 6
[15] CA Submissions, page 6.

implementation, system integrations, and user lifecycle management. The risks associated with this phase were specifically identified as supporting the applied contingency.

NS Power submits that, while the full contingency amount is not expected to be utilized, maintaining a 15% contingency remains appropriate given the risks associated with the remaining scope. Although these risks have not fully materialized to date and NS Power does not expect to utilize the full contingency, the presence of uncertainty requires that appropriate contingency be maintained to manage the remaining work prudently.

2.4 Total Cost of Ownership

The CA acknowledges that the basis for sustaining operating costs is reasonable and that NS Power has a moderate to high level of confidence in its operating expense forecast. However, the CA expresses concern that NS Power did not identify specific steps taken to minimize ongoing operating costs and submits that this should be considered by the Board.[16]

NS Power actively manages costs throughout the project lifecycle, including the negotiation of ongoing operating costs associated with technology solutions. In this case, a competitive RFP process evaluated multiple vendors across both capital and operating cost components, resulting in preferred pricing and the selection of IBM for Managed Security Services (MSS), alongside Saviynt (IGA) and CyberArk (PAM) SaaS solutions. This process was designed to optimize overall project costs and minimize ongoing operating expenses.

NS Power has provided visibility into the total cost of ownership. In addition to the capital investment, the application includes ongoing costs such as SaaS licensing, Managed Security Services, onboarding, and internal support, which are detailed in Attachment 3 to the application.

[16] CA Submissions, page 6.

3.0 RESPONSE TO SBA SUBMISSIONS

The SBA has identified two principal concerns regarding this application. First, it questions whether the cyber incident contributed to cost increases, the overall value of the Project, and whether the proposed solution is sufficient to prevent similar events. Second, the SBA raises concerns about the relationship between this application and prior IT capital projects, including whether previously approved investments should now be considered no longer used and useful. Ultimately, the SBA submits that the application presents an incomplete picture of the total cost required to achieve full deployment of the modern PAM system, and that a consolidated cost through final deployment should be provided.

NS Power addresses each of these concerns below.

3.1 Value of the Project and Cyber Incident Impacts

3.1.1 Project Costs Are Not Attributable to the Cyber Incident

The SBA notes that the IAM project was first identified in the 2025 ACE Plan (filed prior to the cybersecurity incident) and raises concern as to whether any forecast cost increases are attributable to post-incident revisions. [17]

The project was identified in the 2025 ACE Plan as a subsequent submittal, indicating that NS Power intended to advance the project in 2025, but that the scope and estimates were preliminary and not sufficiently developed to support a request for Board approval. In NS Power's updated Q3 Capital Reports (filed as Appendix C to the 2026 ACE Plan), the project was deferred due to the cyber incident, as resources were reallocated to priority restoration efforts. As a result of this deferral, the project was again included in the 2026 ACE Plan as a subsequent submittal, reflecting that it had not yet reached an appropriate level of scope and estimate refinement for approval.

[17] SBA Submissions, page 3

As explained above in Section 2.2 and in the application, the increase from the 2026 ACE Plan subsequent submittal estimate is attributable to continued project development and the evolution of the NIST Cybersecurity Framework, as well as advancements in available technology since the prior estimate was prepared. Incremental costs were driven primarily by higher consulting and labour hours required for additional design, validation, and implementation activities to align with the Company's CSF. As previously confirmed by NS Power, while the cyber incident impacted the project schedule, it did not contribute to the increase in costs.

3.1.2 Value of the Project

The SBA asks whether "everything that is being proposed is sufficient to avoid a similar cyber breach event from occurring again" and questions the "additional protection value" provided by the significant investment contemplated in this application. It further asserts that, while "the complexity of the new systems being added is significant," complexity alone does not demonstrate value or fully address ongoing cybersecurity concerns.[18]

NS Power acknowledges these concerns. While no investment can eliminate the possibility of a future cyber incident, the value of this investment is demonstrated by the capabilities it enables and the risks it addresses. The IAM project is designed to implement a comprehensive, enterprise-wide identity and access management strategy by integrating Saviynt for IGA with modern PAM solutions. Together, these systems enable automated access lifecycle management, stronger security controls, improved compliance, and a more efficient user experience.

The project addresses critical cybersecurity vulnerabilities by replacing an outdated, on-premises PAM solution that exited vendor support in 2025 and reaches end of life in 2026. The cybersecurity landscape has evolved significantly in recent years. Where organizations once relied on protecting the network perimeter, threat actors now target identities, particularly privileged accounts. This

[18] SBA Submissions, page 3.

trend is expected to accelerate as threats become faster, more sophisticated, and increasingly automated through artificial intelligence. In this environment, identity becomes a core security control. This project enables NS Power to reduce risk, enforce least-privilege access, and maintain continuous control in a dynamic threat landscape. It introduces modern PAM capabilities, including protection of high-value credentials, automated credential lifecycle management, password vaulting, and continuous monitoring and session recording. These capabilities are necessary to meet evolving regulatory and industry standards. Without them, NS Power would face higher compliance risk and greater vulnerability to unauthorized access to customer information and critical operational systems.

The transition to IBM's Managed Security Services (MSS) further strengthens this approach by providing access to specialized expertise and supplementing internal capabilities with continuous, 24/7 support. This partnership supports stronger governance and enables the ongoing identification of control gaps and emerging risks, continuous improvement of IAM processes, access to specialized threat intelligence, and operational efficiencies through automation. It also allows for regular benchmarking against industry best practices, ensuring that the IAM program continues to evolve over time.

The project also creates a flexible, cloud-based foundation for future identity-focused security improvements, allowing NS Power to add new capabilities over time and adapt to changing regulatory requirements without replacing the system.

3.2 Prior PAM and IAM Projects

The SBA's second concern relates to prior IAM and PAM capital projects and whether those investments remain used and useful. The SBA questions the relationship between this application and previously approved IT capital projects of similar scope and magnitude, including whether

any components of existing systems can continue to provide value and whether assets not yet fully depreciated should now be considered no longer used and useful.[19]

The assets created by CI C0068714 will replace those associated with CI 49094 and CI C0054455, which relate to earlier PAM implementations based on an on-premises system now reaching end of life. This application replaces that system with a modern, cloud-based PAM solution, CyberArk Privileged Cloud, and introduces new IGA capabilities through Saviynt.

NS Power confirms that no components of the existing system can be reused. The legacy PAM solution provided significant value throughout its operational lifecycle, delivering privileged access controls, security oversight, and compliance support that helped protect critical systems and meet business requirements. However, vendor support for the solution ended in 2025, and the solution will reach end of life in 2026, meaning it will no longer receive security updates or technical support. In addition, the legacy system was built on an older on-premises, self-hosted, architecture that is fundamentally different from the modern cloud-based IAM platform. Any attempt to integrate, extend, or reuse components of the legacy system would introduce significant security risks while increasing implementation complexity and ongoing maintenance requirements. For these reasons, retaining any part of the existing system is not considered feasible.

With respect to the SBA's concerns, the treatment of prior PAM assets is governed by the amortization accounting framework approved by the Board in the 2026–2027 GRA, as discussed in **Section 2.1.3**. Under this framework, the assets associated with CI 49094 and CI C0054455 will continue to be amortized over their approved service periods and will not be retired early for accounting purposes. Upon full amortization, they will be retired in accordance with Accounting Policy 6420, and no unrecovered net book value will remain.

[19] Ibid.

3.3 Project Status

The SBA's final assertion is that this application provides an incomplete picture of the IAM project, particularly with respect to total cost, timing of full deployment, and near-term cybersecurity value. While acknowledging that phased deployment may be necessary, the SBA submits that NS Power should provide a consolidated estimate of the total cost to reach full deployment.[20]

NS Power respectfully submits that this characterization is inaccurate. The scope and total cost of the project have been clearly defined. The work consists of six releases (R1 through R6), which collectively deliver PAM capabilities across key networks, additional CyberArk functionality, and new IGA capabilities through Saviynt. The total project cost is $6,756,522, as set out in the application, and represents the full capital investment required to deliver all in-scope capabilities. Release One was placed in service in February 2026, and the remaining releases are forecast to be completed by August 2026, with a final cost date of April 2027. Approval is therefore sought for the complete scope and cost of the project as described.

NS Power has also provided visibility into total cost of ownership, as mentioned above. In addition to the capital investment, the application includes ongoing costs such as SaaS licensing, Managed Security Services, onboarding, and internal support. These costs were detailed in Attachment 3 to the application.

The project is already delivering meaningful value. Core PAM capabilities, including credential vaulting, automated credential rotation, and controlled system access through SIA, have been in service since February 2026. These controls reduce credential risk and strengthen oversight of privileged access. Additional capabilities continue to be deployed, providing incremental and measurable security improvements with each release. Further enhancements will include Endpoint

[20] SBA Submissions, page 3.

Privilege Manager (EPM) to enforce least-privilege access on workstations and servers, and expanded cloud security capabilities to extend PAM controls across hybrid environments.

Phased deployment is both appropriate and necessary for a project of this complexity. It reduces implementation risk, supports testing and stabilization at each stage, minimizes disruption to critical operations, and ensures that lessons learned are incorporated into subsequent releases. It also allows value to be delivered incrementally, rather than only at project completion. Attempting to deploy all capabilities at once would increase risk, extend timelines, and likely increase overall cost.

Finally, this application relates only to the project described above. The project will be fully deployed upon completion of the six releases in August 2026, at which point the foundational IAM and PAM capabilities will be operational. Ongoing onboarding of additional users and systems will continue as part of normal operations. Any future work beyond the scope of this project, including the implementation of new capabilities, would be brought forward separately for approval, as appropriate.

4.0 CONCLUSION

NS Power submits that the capital expenditures outlined in this application are reasonable, prudent, and in the best interest of customers.

This project is necessary to maintain effective cybersecurity controls and to position NS Power to meet evolving operational and cybersecurity requirements.

NS Power respectfully requests that the Board approve CI C0068714 IT - Identity & Access Management as filed.