Request IR-1:

What is NS Power's threshold for classifying an account high-risk?

(a) How many high-risk accounts does NS Power manage?

Response IR-1:

NS Power has identified high-risk accounts based on [redacted].

High-risk accounts include, but are not limited to, [redacted].

(a) The Company has identified [redacted]. The total number of accounts [redacted] is not able to be disclosed, as disclosure of these specific totals represents significant cyber security risk to NS Power.

Request IR-2:

What does this solution replace?

(a) Is the current Identity and Access Management used by NS Power at the end of its useful life?

(i) If so, when did it reach the end of its useful life?

(a) What steps did NS Power take to sustain the current Identity and Access Management?

(ii) If not, when will the current system reach the end of its useful life?

Response IR-2:

The solution replaces an old on-premises PAM solution that was nearing end of life, as the solution was out of vendor support in 2025 and thus expected to be end of life in 2026. [redacted]

(a) Yes. The assets created by this project will replace those created by CI 49094 IT - Privilege Access Management (PAM) & CI C0054455 IT - Privileged Access Management (PAM) Phase 3.

Identity and Access Management (IAM) as a whole at NS Power is not implemented as a single, standalone platform. Rather, IAM is a combination of processes, policies, and supporting technologies, and PAM is one of those technologies. As such, IAM as a

capability or process does not have a defined "end of useful life" in the same manner as a software system.

(i) Please refer to response above.

(a) NS Power took steps to sustain current and active Identity and Access Management, and NS Power conducts process standardization, implements governance controls, implements security enhancements, optimizes current access management tools all through incremental improvements.

(ii) Please refer to part (a).

Request IR-3:

Please describe any operational efficiencies that will be gained through the investment in a new Privileged Access Management (PAM) system.

(a) Please describe the operational inefficiencies to be incurred resulting from a new PAM system.

Response IR-3:

Benefits of investment in a new PAM system include stronger privileged credential control, centralized vaulting, improved audit evidence, controlled access fulfillment, reduced manual/person-specific dependency, and improved supportability.

(a) NS Power does not expect to experience any major inefficiencies during the implementation, but inefficiencies during transition may include onboarding effort, training, new request routing, documentation/evidence discipline, and temporary process overhead.

Request IR-4:

What type of support will NS Power receive following implementation?

(a) Please describe how the managed support capabilities from operational support services will augment NS Power's existing staff.

(b) How many updates does NS Power anticipate the software performing up to 2034?

Response IR-4:

Following implementation, NS Power will transition to a Managed Security Services (MSS) operating model, under which the vendor provides ongoing operational, maintenance, and continuous improvement support for the IAM environment, including PAM, EPM, IGA, and related access management platforms.

(a) MSS will augment NS Power's cybersecurity posture by performing in-scope IAM operational execution and support through defined queues, runbooks, ServiceNow processes, and escalation paths. NS Power retains approval, governance, prioritization, and accountability. IAM processes in NS Power prior to onboarding MSS were largely decentralized and manual.

(b) This is a SaaS solution deployment where updates will be implemented by the vendor based on new requirements, features, or patches with NS Power being notified via service bulletins. The number of updates is unknown at this time but is anticipated to have limited impact on operations and cost to NS Power.

Request IR-5:

Pages 1 and 2 of the application describe the Identity and Access Management (IAM) framework as a partnership to operate and maintain IAM practices which will effectively allow NS Power to outsource elements of cybersecurity.

(a) Please confirm that this investment is a service that NS Power is investing.

(i) If not confirmed, please explain how this investment is a partnership.

(b) Will Saviynt have control over NS Power's data?

(c) What protections will be in place to stop any unauthorized access to NS Power's data by Saviynt?

(d) Are the support and services from Saviynt based in Canada or the United States?

(i) If so, please describe the risk mitigation strategies NS Power is using to protect the utility's data.

(e) Will the purchase of this framework limit NS Power's future purchases to software supplied by Saviynt?

Response IR-5:

(a) Confirmed. NS Power is capitalizing the costs required to integrate this Software as a Service platform with its existing IT environment, in accordance with Accounting Policy 6215 – Capital Expenditures – Computer Hardware, Software and Telecommunications Equipment.

(b) No. NS Power owns and controls all of the Company's data and remains the data controller under applicable data protection laws. Saviynt operates strictly as a data processor, has no access to the data other than to process it as agreed, and obtains no rights to NS Power's data.

(c) Saviynt enforces zero standing access for all personnel. If support is needed, Saviynt staff must use NS Power's Privileged Access Management (PAM) system to request access using dedicated, credential-less service accounts. This access requires explicit approval from NS Power tied to a valid support ticket, [redacted].

(d) Saviynt delivers services and support from both Canada and the United States. Additionally, NS Power utilizes a technical support center in India to ensure continuous availability during weekends, overnight, and holidays as necessary.

(i) [redacted]

(e) No.

Request IR-6:

When this project was deemed in service, in February 2026, was the project fully implemented or is there work remaining before the project is considered to be fully implemented?

(a) Please describe how NS Power managed the implementation of the project and discuss how and why the implementation management was outsourced to a consultant.

Response IR-6:

The remaining work includes completion of additional PAM capabilities into the corporate environment, along with continued rollout and maturation of EPM, IGA, and associated IAM capabilities, including onboarding of corporate assets, applications, identities, and transition into steady-state managed services

The project in its entirety has not been fully implemented. NS Power implemented the CyberArk Privileged Cloud (PAM tool) enabling privileged account vaulting and automatic password rotation. [redacted] NS Power also transitioned some of the existing identity management practices to the Managed Security Services team (new partner), such as manual provisioning and Access management.

(a) NS Power provided a project management resource to work directly with the vendor's project management team. Below are the responsibilities of each party:

- Vendor PM: Executes and manages the project
- NS Power PM: Enables and supports the project internally

Implementation management was first outsourced to a consultant project manager for staff augmentation at NS Power but was transitioned to an internal project manager in November 2025.

Request IR-7:

Page 2 of the application explains that the selected approach was chosen through a competitive procurement process.

(a) Please provide the quotes received for all proposals.

(b) Please provide the documentation used in evaluating the proposals.

(c) Did NS Power perform a reference check with Saviynt's other customers?

(i) If not, why not?

(ii) If so, please explain the review and evaluation.

(iii) Did NS Power staff test the platform before selecting this vendor?

(d) Please elaborate as to how this IAM is the only feasible option for NS Power.

(i) Identify how alternative IAM frameworks are not as cost effective.

(ii) Please explain how this IAM is the only option that meets the National Institute of Standards and Technology's Cyber Security Framework.

Response IR-7:

(a) Please refer to Confidential Attachments 1-4.

(b) Please refer to Partially Confidential Attachment 5.

(c) NS Power conducted reference checks on the shortlisted vendors. Saviynt is a product of the vendor.

(i) N/A.

(ii) The vendors provided references, which NS Power contacted for feedback. The customers contacted for the reference check indicated the customers' experience with the selected vendor was more positive and that this vendor would be more suited to meet the needs of NS Power.

(iii) The solution was outlined in Demonstration and Oral presentations; however, NS Power did not test the solution.

(d) The chosen bid by IBM is the only feasible option for NS Power because [redacted]

(i) As outlined in Partially Confidential Attachment 5, the IBM proposal [redacted]

(ii) It cannot be confirmed that the IAM framework proposed by IBM is the only solution that meets the National Institute of Standards and Technology's Cyber Security Framework, but based on the proposal and assessment by NS Power SMEs, it was the best overall alternative for NS Power.

C0068714 IR-7 Confidential Attachments 1-4 have been removed due to confidentiality.

Nova Scotia POWER An Emera Company

RFP-08/2024-350 - IAM - Identity and Access Management Services/Solution

Project Overview

Project Details	
Reference ID	RFP-08/2024-350
Project Name	IAM - Identity and Access Management Services/Solution
Project Owner	Ron Fox
Project Type	RFP
Department	IT - Operations
Budget	$[redacted] – an application will be made for additional funding
Project Description	Nova Scotia Power Inc. (NSPI) and Tampa Electric Company Inc (TECO) are seeking proposals on behalf of all Emera Canadian and Emera US companies. There is a significant synergies resulting from both affiliates working together to achieve this objective. Specifically, NSPI and TECO are prioritizing the following three scopes: • Managed Service for the existing Privilege Access Management (PAM) solution (CyberArk) within NSPI, including required upgrades and additional onboarding of assets, as well as a new implementation and Managed Service of CyberArk within TECO. • Managed Service for existing manual Identity and Access Management (IAM) controls and processes within both NSPI and TECO including the implementation of automation.

	• **New implementation and Managed Service of an Identity Governance and Administration (IGA) solution for both NSPI and TECO.** **There is a future need to expand these scopes into the operational technology (OT) environment, showcasing experience in OT within this RFP response would be considered an asset. Our goal is to partner with a provider who can offer reliable, scalable, secure, and cost-effective solutions tailored to our current and future needs, with a vision of continuous improvement in product and service. Partner to look at all existing processes/tools and introduce operational efficiency.**
Open Date	**Nov 12, 2024 9:00 AM AST**
Close Date	**Dec 06, 2024 1:00 PM AST**

Submitted to:

- Andrea MacKay — Procurement Manager
- John MacDonald — Sr Mgr, Proc & Supply Chain, Procurement & Real Estate
- Geoff Moore — VP, Technology Corp. Information Technology
- Chris Smith — EVP, Finance NSPI Corporate VP Finance
- Chris Heck — VP IT & CIO Tampa Electric Leadership Team

Prepared by:

- Ron Fox — Procurement Specialist

Evaluation/Review Team:

- Michael Gorman — Senior Insurance Analyst, SS Insurance
- Godwin Ikhidero — Risk Security Analyst Data Corp. Sec. & Cyber Risk Mgmt
- Rebecca Lee — Director, Information Security, Corp. Sec. & Cyber Risk Mgmt
- Ian Bagnald — Mgr, Ent Cyber Security Risk Corp. Sec. & Cyber Risk Mgmt
- Kenneth Taylor — Director, IT Operations Corp. Tech. Operations
- Steven Pettipas — Solution Architect Access, Corp. Sec. & Cyber Risk Mgmt
- Sathya Sankara Narayanan — Senior Architect, Corp. Tech. Ent. Architect
- Jason Sizemore — Dir, Information Security, IT Leadership Team
- Mayda Gonzalez — Mgr Enterprise Architecture IT HPC Leadership
- David Maldonado — Security Admin Analyst Lead, IT Information Security
- John Hebb — Senior Analyst, Cyber Security, Corp. Sec. & Cyber Risk Mgmt
- Nazih Mourad — Enterprise Security Architect, IT Enterprise Architecture
- Lionel Dufour — Dir, Cyber Security Governance, SS Office of the CIO
- James Boykins — Lead Enterprise Cyber Risk Mgmt Cybersecurity Governance and Awareness
- Sal DiGiorno (TCO Contributor) — Senior Business Analyst, Corp. Tech Project Mgmt Office

Procurement:

- Ron Fox — Procurement Specialist
- Nikitra King (Review) — Contract Admtr Senior

Reviewers/Advisors:

- Wendy MacInnes — Consultant, Project Manager
- Tony Folkins — VP, Digital Technology SS Office of the CIO

Recommendation:

The Evaluation Team unanimously recommends **awarding** the work outlined in the Identity and Access Management RFP to:

- **IBM Canada**

Nova Scotia POWER
An Emera Company

Opportunity Intent to Bid

Name	Vendors	Intent to Bid	Date Signed	Reason
[redacted]	IBM Canada	[redacted]	[redacted]	[redacted]

Nova Scotia POWER An Emera Company

Submissions

Supplier	Date Submitted	Name	Email	Confirmation Code
[redacted]				
IBM Canada				
[redacted]				

Nova Scotia POWER
An Emera Company

Scoring Summary

Active Submissions

	Total	A - Initial Scoring	A-1 - Delivery Capability	A-2 - Company	A-3 - Business and Technical Requirements	A-4 - Delivery Team	A-5 - Managed Services Capabilities	A-6 - Differentiators	A-7 - Insurance	A-8 - Cyber Risk	B - Demos	B-1 - Understanding of Emera's Objective	B-2 - IAM SOLUTION OVERVIEW/KEY FEATURES and BENEFITS	B-3 - OPERATIONAL SUPPORT /MANAGED SERVICE	B-4 - TECHNICAL and PROJECT ASSUMPTIONS	B-5 - IMPLEMENTATION	B-6 - EMERA USE CASE 1: ACCOUNT ACCESS	B-7 - EMERA USE CASE 2: ACCESS REMOVAL/AUDITS	B-8 - EMERA USE CASE 3: MANAGEMENT & INTEGRATION	B-9 - QUALIFICATIONS and EXPERIENCE
Supplier	[redacted]																			
IBM Canada																				

Eliminated Submissions

	A - Initial Scoring	A-1 - Delivery Capability	A-2 - Company	A-3 - Business and Technical Requirements	A-4 - Delivery Team	A-5 - Managed Services Capabilities	A-6 - Differentiators	A-7 - Insurance	A-8 - Cyber Risk	B - Demos	B-1 - Understanding of Emera's Objective	B-2 - IAM SOLUTION OVERVIEW/KEY FEATURES and	B-3 - OPERATIONAL SUPPORT /MANAGED	B-4 - TECHNICAL and PROJECT ASSUMPTIONS	B-5 - IMPLEMENTATION	B-6 - EMERA USE CASE 1: ACCOUNT ACCESS	B-7 - EMERA USE CASE 2: ACCESS REMOVAL/AUDITS	B-8 - EMERA USE CASE 3: MANAGEMENT & INTEGRATION	B-9 - QUALIFICATIONS and EXPERIENCE
Supplier	[redacted]																		

Prior to evaluation, the Evaluation Team elected to only more forward with Proponents who [redacted], leaving 4.
Once we arrived at the final 4 Active Submissions, a decision was made to only move forward with the top 2 scoring proponents for further consideration. [redacted]

Nova Scotia POWER
An Emera Company

Observations

The evaluation team's unanimous recommendation is IBM as the successful proponent:

[redacted]

As well, IBM [redacted] of this initiative.

References

The Evaluation team conducted reference checks on **IBM** with the following businesses:

[redacted]

Nova Scotia POWER An Emera Company

Based on customer feedback, the Evaluation Team's observation is that [redacted] IBM would be best suited for their needs.
References confirmed that IBM was the best option for this initiative.

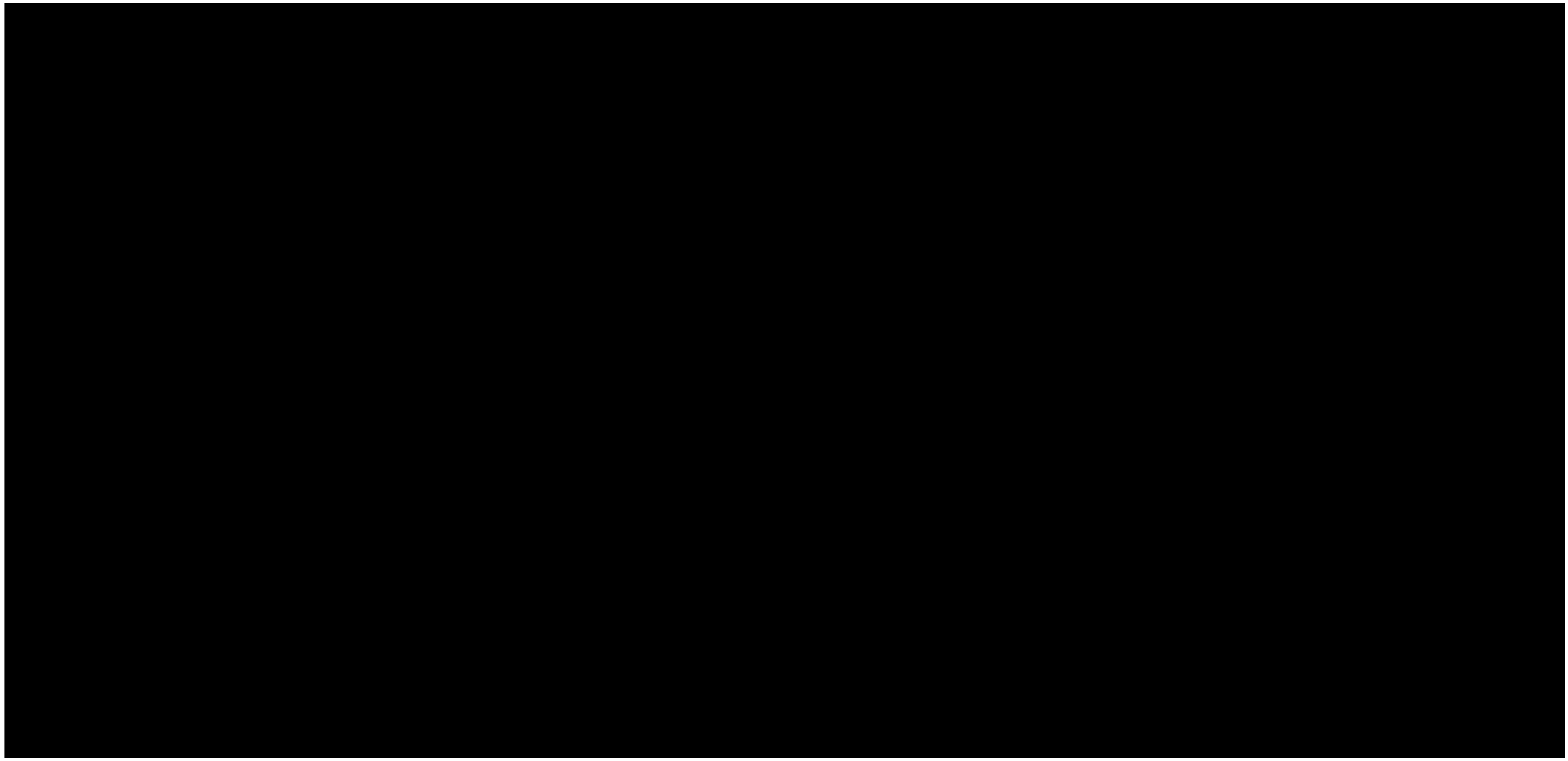
Site Visits

[redacted]

Nova Scotia POWER
An Emera Company

Pricing Comparison

When a successful proponent is selected, the TCO will undergo a final refinement for the Capital Work Order for NSPI's UARB filing and Business Case presentation to TECO Affiliates Presidents.



Nova Scotia POWER An Emera Company

Pricing vs. TCO

[redacted]

Risk:

[redacted]

External cost is subject change based on scope, timeline and contract negotiations.
Internal costs will be adjusted accordingly.

Recommendation:

The evaluation team confidently presents this recommendation to move forward and believes the process was both competitive and transparent and requests senior management approval.

Request IR-8:

In reference to the Capital Project Detailed Estimate:

(a) Please explain the basis of the unit estimate for Regular Labour.

(b) Why is HR/HR IT included in Regular Labour for implementing a capital project?

(c) What is the role of IAM Service Owner and please describe this role in the implementation of this capital investment?

(d) Please describe the Travel Expense incurred.

(e) Does the Estimated Useful Life of 10 years noted on page 1 apply equally to all three licenses - IGA, PAM and WPM?

(f) Please describe the Consulting expenses for Staff Augmentation; RFP Planning and Development; Industry Research/RFP assistance; and Project Management Services (Deloitte).

(i) Please explain why NS Power's internal staff could not perform the following tasks: RFP Planning and Development; Industry Research/RFP assistance; and Project Management Services.

(ii) Please explain the differences between Project Management Services (Deloitte) under Consulting and Project Management under Regular Labour.

Response IR-8:

(a) Please refer to CA IR-5 (a).

(b) HR/HR IT will be involved in requirements gathering, design, user acceptance testing for the IGA implementation of the Saviynt platform. NS Power's HR system will be the source of truth for employee information, integrated with the IGA tool.

(c) The IAM Service Owner is accountable for ensuring the IAM service is operationally supportable, controlled, and aligned with NS Power governance, security, audit, and business requirements. In this capital investment, the IAM Service Owner provides operational input into the future-state support model, validates whether IAM/PAM processes are supportable after implementation, helps define intake, routing, escalation, evidence, and audit-readiness expectations, and identifies operational gaps/dependencies before steady state. Specific roles the IAM Service Owner is responsible for are to oversee the Managed Security Services (MSS) transition from the previous partner to the new NS Power MSS team, to define operational support documentation, and to help define Identity Access workflows to build within the Company's IGA platform.

(d) NS Power visited two vendors during the RFP selection phase to review their Managed Security Services operations. These operations were located [redacted].

(e) Yes.

(f) The descriptions for the Consulting expenses for Staff Augmentation; RFP Planning and Development; Industry Research/RFP assistance; and Project Management Services (Deloitte) are as follows:

- Staff Augmentation – additional consulting staff brought in to augment NS Power internal employees to support project activities, specifically technical and process development activities, for IAM.

- RFP Planning and Development – IT consulting company to plan and develop a request for proposal to go to market for the IAM project. This is a specialized skill set not available internally.

- Industry Research/RFP assistance - Engagement with NS Power's independent technology research and advisory partner to provide independent, vendor neutral research, vendor and cost evaluation, and validation of IAM and managed services approaches against market best practices. This is a specialized skill set not available internally.

- Project Management Services - This external service provided consulting services including governance, control, and guidance to the IAM project team. This support is no longer active or required as an internal project manager has been assigned to the project.

(i) These consultants are experts in the IT and cybersecurity fields, and NS Power required their guidance for the best possible results in the IAM contract selection. NS Power does not have the resourcing or expertise to provide these services.

(ii) Project Management Services provide governance, control, and guidance from an overarching cyber security expert perspective. Project Management under regular labour is an internal NS Power resource (Project Manager).

Request IR-9:

This system will govern the identity lifecycle of approximately 3,500 users, integrate with the Human Resource system and enable external personnel to provision and deprovision access across the enterprise. Please explain why a Privacy Impact Assessment is not applicable.

Response IR-9:

The employee data stored and processed is limited to business contact information and does not extend to include Privacy Impact Assessment.

Request IR-10:

Please provide a copy of Appendix A – Total Cost of Ownership Project Financials – IT – Identity and Access Management in excel format with formulas intact and protections removed.

Response IR-10:

Please refer to Partially Confidential Attachment 1.

C0068714 IR-10 Confidential Attachment 1 has been removed due to confidentiality.

Request IR-11:

The Statement of Work (SOW) states [redacted]

(a) [redacted]**?**

(i) If so, [redacted]**?**

(b) The SOW appears to [redacted]**.**

Response IR-11:

(a) No.

(i) N/A.

(b) Confirmed.

Request IR-12:

The SOW states [redacted].

(a) Which specific [redacted] under this contract are subject to [redacted]?

(b) What process does NS Power use to determine [redacted]?

(c) What is the estimated cost of providing [redacted]?

(i) Please identify where in the detailed project estimate this expense has been included.

Response IR-12:

(a) No [redacted] are subject to [redacted]

(b) N/A.

(c) N/A.

Request IR-13:

[redacted]

(a) If so, how is that [redacted]?

Response IR-13:

Based on the currently defined project scope and supporting documentation, the CyberArk PAM (including Secure Infrastructure Access) implementation [redacted] Systems within [redacted] to CyberArk PAM under this initiative.

[redacted]

(a) N/A.

Request IR-14:

[redacted].

(a) What controls ensure the complete and timely revocation of those credentials?

(b) Is revocation verified by a NS Power independent party or will it solely rely on [redacted]?

(c) To what extent will NS Power's systems and data be accessible to [redacted]?

Response IR-14:

(a) NS Power enforces a combination of preventive, detective, and governance controls to ensure the complete and timely revocation of privileged access granted to IBM personnel during the transition phase:

- Formal Access Governance Processes - All privileged access is provisioned and revoked through controlled workflows within ServiceNow and supporting IAM systems, requiring documented approvals and traceability.

- User Access Reviews (UAR) / SOX (Sarbanes–Oxley)

- Controls - Periodic (quarterly) access certifications are conducted to:

    - Validate that access remains appropriate
    - Identify and remove any excess or orphaned privileges
    - Ensure timely deprovisioning aligned with transition milestones

- Principle of Least Privilege (PoLP) - Access is granted strictly based on role requirements and is continuously monitored to prevent over-privileged access.

- Automated and Manual Deprovisioning Mechanisms

- Access is tied to roles and entitlements that are systematically revoked upon cutover

    - Transition-specific access is time-bound where possible

- Audit Logging and Monitoring - All privileged access activity is logged (via CyberArk and related systems), enabling:

    - Monitoring of credential usage
    - Detection of anomalous access
    - Validation that access is no longer in use post-revocation

These combined controls ensure that access is systematically removed, verifiable, and aligned with governance and compliance expectations.

(b) Yes, revocation will be verified by the NS Power IAM Service Owner to ensure segregation of duties is applied appropriately. Revocation of privileged access does not rely solely on IBM attestation. Rather, NS Power applies independent verification controls to ensure robust oversight:

Segregation of Duties (SoD):
The individual requesting or holding access cannot approve or validate their own access. Approval, provisioning, and validation activities are separated across roles.

Access Certification and Control Evidence:

Periodic access reviews serve as formal evidence of revocation. Audit artifacts (logs, approvals, certification records) are retained for compliance validation.

Alignment with SOX and Internal Audit Requirements:

Controls are designed to meet regulatory expectations, ensuring that access removal is:

- Independently verified
- Fully auditable
- Consistently enforced

This approach ensures that access revocation is objectively validated and not dependent on vendor self-attestation alone.

(c) During the transition and operational support phases, IBM personnel located outside of Canada (e.g., in approved delivery centers) may have access to NS Power systems under strictly controlled conditions. The extent of this access is governed as follows:

Role-Based and Scoped Access:

Access is granted based on specific job functions and operational requirements. Permissions are limited to the minimum necessary systems, environments, and data required to perform assigned tasks.

Controlled Access via Privileged Access Management (PAM):

All privileged access is brokered through secure platforms (via CyberArk and related systems). Direct credential exposure is restricted; session-based access and credential vaulting are enforced.

Security Controls and Restrictions:

IP restrictions and network controls limit access to approved locations. Multi-factor authentication (MFA) is required for privileged access. Session monitoring and recording provide full visibility into activities.

Geographic Access Transparency:

Access is limited to approved IBM delivery locations (e.g., Costa Rica, India) as defined within the operating model. All access is subject to NS Power oversight and audit.

Audit, Monitoring, and Compliance Oversight:

All access activity is logged and subject to review. Any deviations or unauthorized access attempts are investigated. Controls are aligned with contractual, security, and data protection requirements.

Ongoing Governance and Future-State Enhancements:

As IAM capabilities mature (e.g., further centralization and automation), additional controls such as enhanced Role Based Access Controls (RBAC) and identity governance will further refine and restrict access scope

This ensures that access by IBM personnel outside of Canada is controlled, monitored, limited in scope, and aligned with NS Power's security and governance standards.

Request IR-15:

[redacted].

(a) What data residency and sovereignty controls govern NS Power's identity and access data, including Active Directory attributes, privileged account inventories, session recording and audit logs [redacted]?

(b) By how much would the final contract price be increased if the SOW was modified [redacted]?

(i) Did NS Power request this limitation?

(a) If not, why not?

(b) If so, why was it not pursued?

Response IR-15:

(a) IAM data (including Active Directory, audit logs, and session-related data) remains hosted within client-managed infrastructure located in Canada. The vendor, as a managed security service provider, does not host or store this data within vendor-owned systems, and MSS personnel do not persist or store client data locally. However, authorized vendor personnel [redacted] access client systems remotely to support operational functions. Access is performed through controlled mechanisms, [redacted] and all access is subject to Emera's cybersecurity controls (e.g., authentication, logging, monitoring, and privileged access management).

Data remains [redacted].

(b) This was not priced at the time of RFP. As such, the final contract price to include this modification is unknown.

(i) No.

(a) It was not a requirement for the RFP. Please refer to NSEB IR-5 (d) for risk mitigation strategy.

(b) N/A.

Request IR-16:

The SOW permits [redacted]

(a) Does NS Power have a thorough understanding/knowledge of all the jurisdictions from which [redacted] **NS Power systems and/or data?**

(b) Does the [redacted] **NS Power before introducing personnel from a new jurisdiction?**

Response IR-16:

(a) Yes.

(b) No. It is common in global IT services agreements to permit vendors to utilize worldwide delivery resources with a pre-authorization for global staffing.

Request IR-17:

Saviynt is a SaaS platform, meaning NS Power's identity data will reside in Saviynt's cloud infrastructure for contract term. The document does not describe Saviynt's data hosting location, security certifications (ex. SOC 2, ISO 27001), subprocessors or breach notification obligations. What due diligence was conducted on Saviynt's security posture and Canadian data residency?

Response IR-17:

A formal vendor risk assessment will be conducted as part of the project. As part of the RFP process, the vendor provided responses to an initial cyber security questionnaire.

NS Power owns and controls all of the Company's data and remains the data controller under applicable data protection laws. Saviynt operates strictly as a data processor, has no access to the data other than to process it as agreed, and obtains no rights to NS Power's data.

[redacted]

Request IR-18:

[redacted]. **What separation of duty controls prevent** [redacted]**?**

Response IR-18:

NS Power can [redacted]

Request IR-19:

Pages 19 and 20 of 65 (pdf page 74-75) presents the [redacted].

Response IR-19:

Orphan Account Management in Saviynt is a functionality enabling the use of rules to maximize adoption. It is not an activity that is performed by vendor. Saviynt will identify orphan accounts. This is accomplished by using NS Power-defined rules to maximize adoption of accounts to identities. For any accounts that remain orphans (rules cannot find matching identities), NS Power will need to address directly through operational efforts to provide enough data on the accounts to allow for adoption as appropriate, which addresses the assumption in Section 6.1.3 as it is not a task performed by the vendor.

Request IR-20:

[redacted]**?**

Response IR-20:

NS Power's approach [redacted]

From a vendor perspective, RBAC is a significant effort which is out of scope for the initial phase of the IGA solution deployment. Role mining within Saviynt can be performed by the Managed Security Services Provider at the direction of NS Power after the application account and entitlement data is loaded for applications of interest. The vendor's focus within this project is solely on determining the default access rights that a user should automatically receive when they first join the organization (or take on a specific role), also known as birthright access.

Request IR-21:

[redacted]. **The accuracy of all downstream automated provisioning and deprovisioning depends on the timelines and the quality of data in those systems.**

(a) What is the current state of identity data quality with these sources?

(b) Please provide an example where [redacted].

(c) Will inaccurate data be extended into this implementation?

Response IR-21:

(a) Prior to the cyber event, a data file was exported nightly from PeopleSoft (PS) and imported into Active Directory (AD) with the latest employee information such as Manager, End Date, and Employment Status. This employee data would then sync to ServiceNow from AD. Depending on the employment status, it would auto-order catalog items such as Offboarding, Leave of Absence, etc. [redacted] the Company created catalog items visible to the HR teams only to mimic this nightly data file export and sync process. For example, should HR submit an "Offboard Employee" catalog item, the task would go to the PS group to manually update the employee in PS, and the employment status in ServiceNow will subsequently be updated to trigger an auto-order of the necessary IT Offboarding.

(b) On April 25, 2026 an offboarding request was submitted in NS Power's enterprise workflow platform. This triggers multiple tasks for various teams to remove various forms of access (physical access, identities, accounts (privileged and non-privileged as

applicable), email, etc.) These teams would action these tasks and update the request accordingly. In this specific example, all tasks were completed and the request was fulfilled and closed on April 29, 2026.

(c) All data is being vetted prior to use in the implementation, though much of this validation is currently performed through manual processes. As key functionalities are rebuilt—such as the integration between PeopleSoft and Active Directory—these validation and maintenance processes will be automated, ensuring ongoing data accuracy and consistency.

Request IR-22:

Pages 54-55 (pdf page 109-110) describes [redacted]. How has NS Power defined [redacted]?

(a) Does that definition explicitly cover scenarios such as [redacted]?

Response IR-22:

Priority 1 (P1) incidents (and all incidents, P1-P4) are defined with this grid:

Urgency / Impact	Enterprise Wide	Critical Site / Department	Group of Users	Single User
Unable to work / Cannot perform job function	P1	P1	P2	P3
Work Disrupted / Cannot perform portion of job function	P1	P2	P2	P3
Slight Disruption / Can still perform job function	P2	P3	P3	P4
Minor Inconvenience	P3	P3	P4	P4

(a) Grid Emergency or Cyber incidents would be defined by either Enterprise-wide urgency/impact, or Critical site/department urgency/impact, and would constitute a P1 incident assignment.