

CI C0085287

**IT - Cybersecurity Standard Integrated Platform
Program**

REDACTED

October 5, 2026





NSEB APPROVAL SHEET

Project Title: IT - Cybersecurity Standard Integrated Platform Program

CI Number: C0085287

Date: October 5, 2026

Expenditure Profile			Type of Filing	
Year	Budget Amount	Project Estimate	☐	Capital Project Authorization
2026		1,689,888	☒	Unforeseen and Unbudgeted (U&U)
2027		251,632	☐	Planned & Advanced (P&A)
			☐	Subsequent Approval Item
			☐	Authorization to Overspend (ATO)
			☐	Scope Change
			☐	Final Cost (FIN)
Total	\$0	\$1,941,520		

COMMENTS

Submitted on behalf of NOVA SCOTIA POWER INCORPORATED

Authorized Signatory
Dave Pickles
Chief Operating Officer

DATE
October 5, 2026

Approved on behalf of NOVA SCOTIA ENERGY BOARD

DATE

CI Number: C0085287

Title: IT - Cybersecurity Standard Integrated Platform Program

Start Date: 2026/07
 In-Service Date: 2026/10
 Final Cost Date: 2027/10
 Function: General Plant
 Forecast Amount: \$1,941,520

DESCRIPTION:

This project will implement [REDACTED] as NS Power's primary cybersecurity platform for the IT environment and transition away from several legacy tools and services, including [REDACTED] and [REDACTED]. The work includes the planning, design, implementation, transition, and decommissioning activities required to deploy the platform, retire overlapping tools where appropriate, and establish a more standardized cybersecurity operating model.

The platform will consolidate capabilities such as threat detection and response, vulnerability visibility, data protection, cloud security, exposure management, and related managed detection and response activities. Existing tools will be replaced where [REDACTED] can meet NS Power's business and technical requirements, while select, specialized solutions will be retained only where critical capabilities cannot be effectively replaced. Final tooling decisions will be informed by technical recommendations and approved by NS Power cyber leadership.

The intended outcome is improved cyber visibility, threat intelligence, faster response, reduced operational overhead, and stronger cyber risk management across the IT environment. Operational Technology (OT) implementation is excluded from this project and will be addressed separately.

Summary of Related CIs +/- 2 years:

Pursuant to Section 11.2 of the CEJC, related CIs for General Plant projects include "Work completed on the same asset (application, building, etc.)."

- 2025 – C0061284 – IT – OT Cyber Security Control Implementation \$6,826,426

Depreciation Class: General Plant – Office Furniture and Equipment – Computer Software

Estimated Life of the Asset: 10 Years

JUSTIFICATION:

Justification Criteria: Information Technology Application and Hardware System

Sub-Criteria: Technical

Why do this project?

NS Power needs to complete this project because cybersecurity threats continue to increase in volume and sophistication, including threats supported by agentic AI, and generative AI. The current cybersecurity environment relies on multiple tools, vendors, contracts, and support models, creating operational complexity and limiting the consistency, visibility, and speed of security operations.

The project strengthens NS Power's cybersecurity risk posture by improving threat intelligence, threat detection, incident response, vulnerability visibility, data protection, cloud security, and exposure management across the IT environment. Moving to a more integrated platform will help NS Power identify, investigate, and respond to threats more quickly, reduce control gaps, and support more informed, risk-based decision making.

The project also provides operational and financial benefits through technology standardization, vendor rationalization, and reduced reliance on periodic cybersecurity assessments. [REDACTED] will provide more continuous visibility into cyber risk exposure, control effectiveness, and security gaps, helping shift NS Power from periodic point-in-time assessments toward a more current and actionable understanding of cybersecurity risk.

Why do this project now?

Several critical cybersecurity tool licenses and services expired on September 30, 2026, requiring a decision on the future direction of the cybersecurity technology portfolio. Rather than renewing a collection of disparate legacy tools, this project provides an opportunity to transition to a more integrated cybersecurity platform that improves real time threat intelligence, operational efficiency, strengthens security capabilities, and reduces technology complexity while maintaining essential protections for the organization.

Proceeding now will help maintain uninterrupted cybersecurity coverage, reduce the risk of overlapping technologies, and accelerate the operational benefits associated with tool consolidation.

Technology consolidation and vendor rationalization are expected to avoid approximately \$0.4 million annually, or approximately \$1.2 million over three years, in service and licensing costs, subject to final confirmation of tool retirement and contract transition activities.

The timing also allows NS Power to implement enhanced capabilities that are not fully available through the current toolset, including enhanced threat intelligence, exposure management, file integrity monitoring, incident response retainer services continuous threat hunting, and training credits. Delivering these capabilities alongside planned decommissioning activities supports a cleaner transition and reduces the likelihood of paying for overlapping tools longer than necessary.

If the project is deferred, NS Power's existing tools risk being outpaced by frontier AI enhanced attack capabilities and the Company's cyber defenses are likely to become inadequate at protecting its business and the critical infrastructure required to serve its customers.

Why do this project this way?

NS Power considered whether to continue with the existing cybersecurity operating model by renewing the current tools and services. While this option would reduce near-term implementation effort, it would maintain reliance on multiple vendors, technologies, contracts, and support models, and would limit opportunities to accelerate the Company's response to threats, better understand threats, improve integration across different defenses, improve visibility, and gain efficiencies and standardization.

NS Power also considered whether existing technologies already deployed in the environment, including Microsoft and Tenable solutions, could be expanded to meet the project objectives. These platforms remain important parts of the cybersecurity ecosystem; however, they are not sufficiently comprehensive solutions.

The recommended approach is to implement the [REDACTED] platform-based solution because it puts NS Power in the best position to keep pace with the leaps in expertise and attack capabilities of threat actors using generative AI and agentic AI capabilities. The decision considered breadth of cybersecurity functionality, integration with existing technologies such as ServiceNow, support for future IT and OT use cases, opportunities for vendor consolidation, operational efficiency, scalability, and overall value.

This approach consolidates multiple cybersecurity functions onto a single integrated platform, which reduces operational complexity, improves visibility across the IT environment, strengthens telemetry correlation across security domains, improves the time between threat identification and response action, and enables a more coordinated approach to threat detection, investigation, response, and cyber risk management.

Contingency Statement

Contingency for this project has been determined using a combination of internal subject matter expert judgment (Project Managers, Business Analysts, Financial Analysts, Cyber Security Professionals, and Technical Leads) and the non-binding contingency guidelines. Consistent with the Decision Gate (DG) process described in the non-binding contingency guidelines, a 15 percent contingency has been applied. Based on the current level of project definition and maturity, this project is being filed as DG4. Risks intended to be covered by the contingency include cost uncertainty and unforeseen effort that may arise as implementation progresses, including integration and collection of logs from non-standard source systems, endpoint (servers, desktops and laptops) sensor agent deployment support, legacy tool decommissioning, and unforeseen technology risks that may arise during build activities.



Instructions: Select option in Column B.
Columns C through G will auto-populate.

Document No: XXX-XX-XXXX-XXXX

Project Cost Estimate Input Checklist and Maturity Matrix						
Equipment Replacement		Required fields:		Estimate Classification		
Project Name: IT - Cybersecurity Standard Integrated Platform Program		Started or Preliminary	Class 5	Class 4	Class 3	Class 2
Maturity Level of Project Definition Deliverables		Defined or Complete				Class 1
General Project Data						
A. Scope						
Project Scope of Work Description	Defined (D)	P	P	D	D	D
B. Capacity						
Not Applicable	Not Applicable (NA)					
C. Project Location						
Hardware (server, network infrastructure)	Defined (D)	P	P	D	D	D
D. Requirements						
Codes and/or Standards	Defined (D)	NR	P	D	D	D
Legislative Requirements	Not Applicable (NA)	NR				
E. Technology Selection						
Design/Technology	Defined (D)	NR	P	D	D	D
F. Strategy						
Contracting/Sourcing	Defined (D)	NR	P	D	D	D
Escalation	Defined (D)	NR	P	D	D	D
G. Planning						
Logistics Plan	Defined (D)	P	P	P	D	D
Integrated Project Plan	Defined (D)	NR	P	D	D	D
Project Code of Accounts	Defined (D)	NR	P	D	D	D
Project Schedule	Defined (D)	NR	P	D	D	D
Regulatory Approval & Permitting	Preliminary (P)	NR	P			
Risk Register	Defined (D)	NR	P	D	D	D
Stakeholder Consultation/Engagement/Management Plan	Defined (D)	NR	P	D	D	D
Work Breakdown Structure (WBS)	Defined (D)	NR	P	D	D	D
Start-up & Commissioning Plan	Defined (D)	NR	P	P/D	D	D
Technical Deliverables (Specifications and/or Drawings)						
Network Infrastructure	Complete (C)	P	P	C	C	C
Data Architecture	Complete (C)	P	P	C	C	C
Security Assessment	Defined (D)	NR				
Privacy Impact Assessment	Not Applicable (NA)	NR				
Information Systems/Telecommunication Drawings	Complete (C)	NR	P	C	C	C
Total Responses		Total # Deliverables for this Project	5	18	17	17
Percentage		% Defined/Complete towards Class Estimate	100%	95%	89%	89%

Comments:

While AACE does not provide guidelines for Information Technology (IT projects), industry best practices such as PMI's Practice Standard for Project Estimating recommend IT projects follow a Risk base work cycle like a Decision Gate (DG) process where the project scope, schedule and budget are continuously defined over a series of decision gates. This project is filed at DG4 with a contingency level consistent with that stage of the project. The maturity checklist completed above demonstrates that the majority of the project deliverables have been defined. This project measured 89% of deliverables defined or completed for a Class 3 estimate.

Legend:

The maturity level is an approximation of the completion status of the deliverable. The completion is indicated by the following descriptors:

General Project Data:

- Not Required (NR): May not be required for all estimates of the specified class, but specific project estimates may require at least preliminary development.
- Preliminary (P): Project definition has begun and progressed to at least an intermediate level of completion. Review and approvals for its current status has occurred.
- Defined (D): Project definition is advanced, and reviews have been conducted. Development may be near completion with the exception of final approvals.

Technical Deliverables:

- Not Required (NR): Deliverable may not be required for all estimates of the specified class, but specific project estimates may require at least preliminary development.
- Started (S): Work on the deliverable has begun. Development is typically limited to sketches, rough outlines, or similar levels of early completion.
- Preliminary (P): Work on the deliverable is advanced. Interim, cross-functional reviews have usually been conducted. Development may be near completion except for final reviews and approvals.
- Complete (C): The deliverable has been reviewed and approved as appropriate.

Note: This checklist is intended to be used for IT/OT projects. In lieu of specific AACE guidelines for these types of projects, this checklist was developed by NS Power following the principles of the guidelines to demonstrate confidence in the cost estimate maturity.

Project costs must be detailed by major project phase and would normally align with a potential stage-gate (i.e. preliminary design, initial scoping, requirements, etc.). Within each phase, major cost items must be identified. The tables may be expanded to include additional phases if required and columns may also be added if it is necessary to include additional fiscal years.

[illegible]

Sustaining Operating Costs (gross)	OPEX	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Licensing and Services	OPEX										
Operating & Maintenance Services	OPEX										
Total Sustaining Operating Costs	\$ 4,734,992	\$ 295,937	\$ 1,775,622	\$ 1,775,622	\$ 887,811						

Savings		2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
Endpoint Detection and Response Platform	OPEX	\$ 237,495	\$ 1,640,971	\$ 1,640,971	\$ 820,485	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
Third Party Cybersecurity Provider	OPEX	\$ 104,152	\$ 624,909	\$ 624,909	\$ 312,455	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
Third Party Cybersecurity Provider	OPEX	\$ 21,667	\$ 130,000	\$ 130,000	\$ 65,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	OPEX	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
		\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
Total Savings		\$ 6,353,014.00	\$ 363,314	\$ 2,395,880	\$ 2,395,880	\$ 1,197,940					

Note to Authors: Table A.4 Lines 7 through 9 are populated automatically from Tables A.1 through A.3

[illegible]

REDACTED (CONFIDENTIAL INFORMATION REMOVED)

**CI C0085287 Confidential Attachment 1 has been removed
due to confidentiality.**