National Cybersecurity Consortium

Corporate Plan
2026-2027

NATIONAL CYBERSECURITY CONSORTIUM
CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

www.ncc-cnc.ca

Part 1
Executive Summary

The National Cybersecurity Consortium (NCC) is a not-for-profit organization dedicated to advancing Canada's cybersecurity ecosystem through research and development, commercialization, and training.

Created in 2021 by centres of cybersecurity expertise at five Canadian universities – Concordia University, Toronto Metropolitan University, the University of Calgary, the University of New Brunswick, and the University of Waterloo – the NCC is responsible for distributing funds from the Government of Canada's Cyber Security Innovation Network (CSIN), a program of the Ministry of Innovation, Science and Economic Development (ISED). The NCC has confirmed commitments of more than $55m in grants to Canadian cybersecurity projects through fiscal 2025-2026.

Strategic Approach

The NCC has built its operational capacity and its reputation within the Canadian cybersecurity ecosystem through three distinct strategic phases:

1. **Phase One – Building the Foundations** (Spring 2022 through Fall 2023): the NCC focused on identifying and establishing the critical operational elements required to deliver on the NCC's vision, mission, and programs.
2. **Phase Two – Activation** (Fall 2023 through Winter 2025): The NCC has built its core business activities, expanded stakeholder involvement, and has activated NCC program activities and ecosystem engagement.
3. **Phase Three – Full Operations** (Winter 2025 through Winter 2029): The NCC will build on its leadership role in the Canadian cybersecurity ecosystem and solidify engagement, program, and administrative operations.

The NCC looks to build on its role as a leading driver and supporter of Canadian cybersecurity activities:

- Maintaining a strong, accountable **governance** structure
- Continuing strategic and effective **operations**
- Designing and delivering robust **programming and stakeholder engagement**
- Shaping a public presence and delivering strong **communications and ecosystem outreach**

Planned activities to support these objectives in the 2026-2027 fiscal year include:

- Continuing the development of the Board of Directors to reflect a diverse, pan-Canadian approach to cybersecurity
- Activating the Scientific & Ecosystem Advisory Committee (SEAC) to provide advice and insight to the NCC regarding emerging issues in the Canadian and international cybersecurity environments
- Further building and assessing the NCC's administrative and program delivery team

- Continuing a strong and positive working relationship with the Canadian federal government, ensuring mutual insight and understanding of the Canadian cybersecurity ecosystem
- Continuing development of the ecosystem and stakeholder development strategy, including working to continually expand and deliver on the NCC's value proposition and seeking further funds to support research, capacity building and commercialization activities across the ecosystem
- Building on the success of the NCC's 2025 Conference with its 2026 Conference in Montreal.

This Corporate Plan presents expected revenue, planned expenditures, and cash flow requirements, phased by quarter, for the 2026-2027 fiscal year.

Part 2
Introduction

2.1. About the NCC

The NCC is a federally incorporated not-for-profit organization committed to the advancement of Canada's cybersecurity ecosystem. The organization was founded in 2021 by centres of cybersecurity expertise at five Canadian universities: Concordia University, Toronto Metropolitan University, the University of Calgary, the University of New Brunswick, and the University of Waterloo. On February 17, 2022, the Government of Canada committed up to $80 million over four years to the NCC through the Cyber Security Innovation Network (CSIN) program. This funding is a foundational investment that is intended to support the growth of Canada's cybersecurity ecosystem through collaboration amongst academic, not-for-profit, and private sector participants.

2.2. Our vision

The NCC's vision is to advance Canadian cybersecurity innovation and talent development through research, commercialization, and training.

2.3. Our mission

The NCC's mission is to grow a pan-Canadian network that works with private and public sectors to lead world-class cybersecurity innovation and talent development and to increase cybersecurity-related economic activity in Canada.

2.4. Our values

- **Partnership |** We promote and cultivate collaboration and partnership opportunities between academia and the private and public sectors.
- **Growth |** We build innovative cybersecurity systems to establish economic growth and sustainability for Canada and Canadians.
- **Research and Innovation |** We build and sustain robust research and development partnerships with industry.
- **Human Resources Skilled in Cybersecurity |** We support the creation of training programs that meet the true cybersecurity needs of the private and public sectors.
- **Knowledge Sharing |** We create a knowledge-sharing community in which access to expertise is available anytime, anywhere from experts and peers.
- **Inclusion |** We integrate the principles of equity, diversity, and inclusion across all areas of the NCC, and promote an inclusive organizational culture that values diverse perspectives and contributions.

2.5. Our commitment to accountability

In carrying out our mission, the NCC is committed to the highest standards of accountability and transparency.

We adhere to best practices in governance by ensuring that appropriate authorities, accountabilities, and decision-making structures are established. This includes attracting a highly qualified and diverse Board of Directors, articulating clear roles and responsibilities for NCC management and Board members, establishing appropriate Board oversight committees, and ensuring clear and strategic communication between the organization's management and the Board.

Transparency and accountability underpin all NCC operations. Our operations will be guided by key oversight documents and processes, including corporate plans, annual reports, external financial audits, ongoing risk management assessments and responses, and performance monitoring.

2.6. Our focus

The NCC cultivates collaboration and capacity-building in the private and public sectors across five focus areas:

1. **Critical infrastructure protection**: to develop solutions that enable proactive monitoring and real-time detection and mitigation to restore critical infrastructure from damage and interruptions inflicted by cyber-attacks.
2. **Human-centric cybersecurity**: to understand how human factors influence and impact security and privacy requirements in order to develop new human-centric cybersecurity solutions.
3. **Network security**: to develop tools, techniques, and procedures to safeguard computer networks and hosts from both internal and external exploits.
4. **Privacy and privacy enhancing technologies**: to develop protective technologies across many different environments that safeguard individuals and data from privacy violations.
5. **Software security**: to develop tools, methods, and practices to reveal and cure vulnerabilities before software is released to end-users.

2.7. Context

The need for talent development, innovation, commercialization, and collaboration across Canada's cybersecurity ecosystem continues to grow. The increasing adoption of technologies like generative artificial intelligence, potential concerns regarding Canadian sovereignty, and the surge in remote and hybrid work have created emerging threats to Canada's critical infrastructure.

Cybersecurity solutions, products, services, and expertise must keep pace with Canada's digital transformation. The NCC believes this transformation will require significant expansion of shared effort and investment in research, innovation, commercialization, and training across private and public sectors over at least the next decade. We also believe the NCC is well-positioned to provide the leadership that Canada's cybersecurity ecosystem needs to keep Canadians and Canada safe.

The NCC intends to be the leader in catalyzing development, innovation, and collaboration within the cybersecurity community in Canada.

Part 3
Strategic Approach

In the first years of the NCC's operation, the Board of Directors has been focused on building the administrative foundations of the organization to support the delivery of funding programs, and in building a community interested in the understanding and advancement of cybersecurity issues in Canada. The NCC Board has taken a measured approach, prioritizing its activities to effectively align resources and to best ensure organizational success and sustainability for the future.

As the Board transitions from its initial duties of operational oversight to a greater focus on strategic direction, it will ensure pan-Canadian representation, strong governance, and sustainability for the organization.

3.1. Our work

The NCC continues to build its operational capacity and its reputation within the Canadian cybersecurity ecosystem through three distinct strategic phases:

1. **Phase One – Building the Foundations** (Spring 2022 through Fall 2023): the NCC focused on identifying and establishing the critical operational elements required to deliver on the NCC's vision, mission, and programs.
2. **Phase Two – Activation** (Fall 2023 through Winter 2025): The NCC has built an operation able to deliver on core business activities and activate NCC program activities and ecosystem engagement.
3. **Phase Three – Full Operations** (Winter 2025 through Winter 2029): The NCC will further build on its leadership role in the Canadian cybersecurity ecosystem and solidify engagement, program, and administrative operations.

The NCC has been successful in establishing its Board of Directors, including expanding the Board to thirteen representatives from across Canada.

The NCC has also continued to build its public presence, including creating a number of engagement events, and effectively delivered on its 2025 Call for Proposals. An iterative approach to delivering calls in an efficient, concise, and defendable manner has been at the core of the NCC's strategy of continuous program delivery improvement.

The NCC continues to build its public profile and to secure a broader range of strategic partnerships, both inside and outside of the Canadian cybersecurity community.

The NCC will be surveying its stakeholder group and Canadian cybersecurity experts annually to determine how the NCC can best support its stakeholders, and also to better identify those issues and concerns that are "top of mind", helping the NCC stay in front of the changing cybersecurity landscape.

Maintaining close connection with the ever-changing needs of Canada's cybersecurity/privacy ecosystem will, in part, be facilitated by advice received from various stakeholders. To facilitate stakeholder input, the NCC has expanded and redefined the activities of the Scientific and Ecosystem Advisory Committee (SEAC, formerly the Scientific Operations Advisory Committee).

The NCC is committed to the principles of diversity, equity, inclusion, and accessibility. The Skills Matrix used to assess and nominate new Board Directors includes a wide range of equity measures, including gender identity and geographic location. The NCC also requests information from each Ultimate Recipient as to the participation of under-represented groups within each project.

Part 4
Planned Activities

Phase Three: Full Operations (Winter 2025 through Winter 2029)

As the NCC moves into Phase Three of its strategic development, it is expected that administrative size will stabilize, supporting a broader expansion of the organization's profile within the ecosystem.

The NCC will continue to deliver on and grow effective and predictable grant programs, and provide high-quality outreach activities to attract stakeholders, potential Ultimate Recipients, and future grant partners.

Planned activities to ensure a strong, accountable governance structure
1. Shift the focus of the Board of Directors from an operational to a strategic outlook, supporting the long-term vision of the NCC 2. Fully activate the Scientific and Ecosystem Advisory Committee (SEAC) to provide the NCC with guidance and insight into the cybersecurity ecosystem 3. Hold the NCC's second Annual Conference in Montreal, QC in June of 2026

Shifting the focus of the Board of Directors from an operational to a strategic outlook will allow the organization to expand its scope and be a vector for greater cohesion across the Canadian cybersecurity ecosystem.

In alignment with the Board of Directors, and under the guidance of the Scientific Director, SEAC will provide key insights into the needs of Canada's cybersecurity community and serve as a key conduit to buildrelationships that will drive expanded research, development, and commercialization projects across the country.

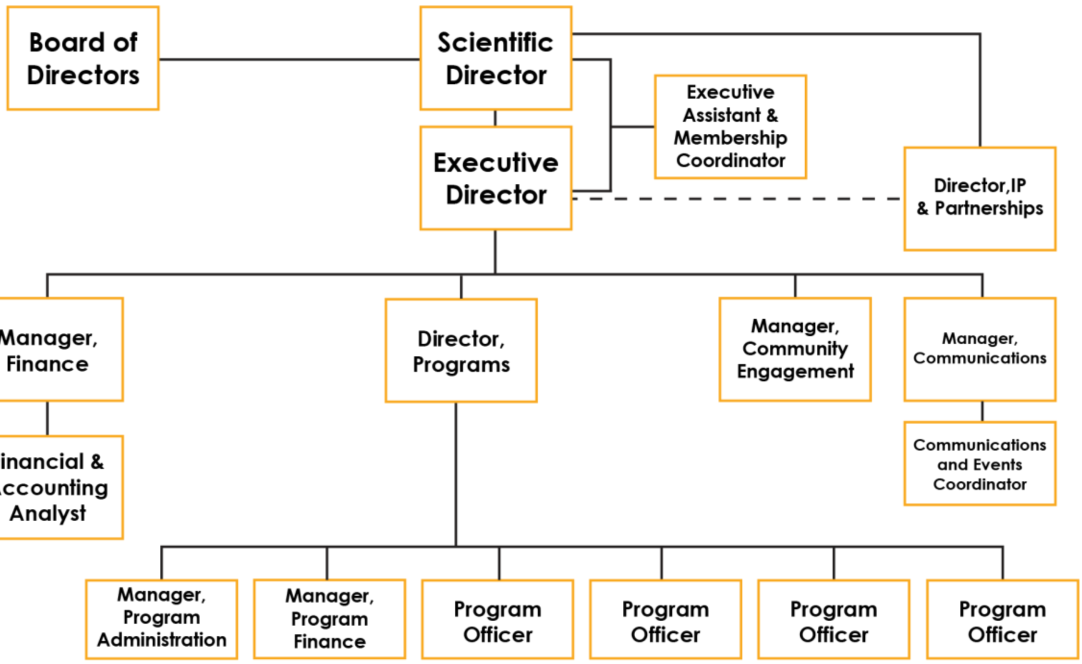
The NCC's second Annual Conference will be held in Montreal in June of 2026, and will seek to capitalize on the success of the NCC's 2025 Conference in Banff, AB.

Planned activities to continue strategic and effective operations
1. Continue the review and improvement of operations, including streamlining project applications and reporting processes 2. Complete the NCC's financial audit and Annual Report for 2025-2026 3. Work collaboratively with Government of Canada and other stakeholders to ensure the long-term sustainability of the NCC to support the Canadian cybersecurity ecosystem

Building an administrative team that is financially sustainable and appropriate for the work being done by the NCC continues to be a priority. The Scientific Director and the Executive Director are continually reviewing the workload of each NCC team and employee.

The NCC's 2025-2026 audit and Annual Report will be completed and ready for presentation to the NCC's Board and Membership at the organization's Annual General Meeting in September of 2026.

Figure 1: Organizational Structure for the NCC – FY 2026-2027



Planned activities to design and deliver exceptional value to the Canadian cybersecurity ecosystem
1. Deliver timely and defendable information on the research outcomes from the 2023, 2024 and 2025 Calls for Proposals 2. Provide regular and ongoing activities for members, including hosting the NCC's 2026 Annual Conference and the 2026 Mastercard Capture the Flag Series 3. Articulate the value of active participation in the NCC and its activities, expand our stakeholder base, and provide exceptional opportunity and value to those stakeholders

The NCC has successfully established itself as an effective and efficient funding agency, streamlining its application process and working to deliver project support funds in a manner that is accountable to the Canadian cybersecurity ecosystem, encouraging growth, innovation, and diversity.

Strengthening collaboration and connections across the cybersecurity ecosystem is central to the vision of the NCC. Ecosystem engagement and outreach will be essential to realizing the NCC's mission to spur world-class cybersecurity innovation and talent development, and to increase cybersecurity-related economic activity in Canada. Creating and supporting such relationships is critical to the long-term sustainability of the NCC. Identifying, engaging, and growing NCC stakeholder involvement among cybersecurity experts, partners, and other ecosystem members from the private and public sectors will be a key priority for the Board, SEAC, and the NCC's administration.

Planned activities to shape a public presence and deliver strong communications and ecosystem outreach
1. Execute and refine the NCC's Communications Plan 2. Increase ecosystem engagement through a growing schedule of events, both in-person and online, including additional conferences, the Mastercard Capture the Flag series, and a potential speaker series 3. Host the 2026 annual conference of the NCC in Montreal

The NCC will have an increasingly active presence on social media, plus an updated website, and will be communicating with stakeholders regularly throughout fiscal 2026-2027.

Part 5
Financial Plan

5.1. Anticipated revenue and planned expenditures for fiscal year (FY) 2026-2027

The NCC anticipates that revenue from ISED and membership fees, balancing planned expenditures for FY 2026-27 for both network and administrative activities will total $21,136 million. It is composed of the following:

- ISED Contribution – Network Activities (Grants) - $16.826 million
- ISED Contribution – NCC Administration - $3.25 million
- Additional Revenues - $1.061 million

5.2. NCC Network Activities - $16.826m

The NCC has successfully completed three Calls for Proposals (2023, 2024 and 2025) plus a top-up call in 2025, supporting projects with more than $55 million in multi-year grants. The value of the 2025 Call for Proposals was $20.9 million, with an additional $1.025 million in top-up funds confirmed, although the final value will be determined by the scope of successfully funded projects. The total value of the projects supported by the NCC in 2025 was $42.605 million, representing a matching ratio (NCC funds to project value) of 1: 0.94.

With an estimated total value of $22.8 million for the 2024 Call for Proposals, it is anticipated that approximately $8.8 million of that total value will be distributed to successful Ultimate Recipients in FY 2026-2027, in addition to roughly $4 million to 2023 projects.

Ultimate Recipient matching funds for the 2023 Call for Proposals totals $28.004 million, for a leverage ratio of 1: 2.48. The estimate of matching funds for the 2024 Call for Proposals is $44.2 million, a leverage ratio of NCC funds of 1: 1:7.

5.3. NCC administration costs ($3.737 million)

The NCC anticipates that resources from ISED and additional revenues (including incremental fees from stakeholders) to support NCC administration costs in fiscal year 2026-27 will total $3.737 million, a small decrease of 1.3% from the previous fiscal year. This decrease is primarily reflected in lower-than-anticipated costs for software and operational infrastructure, while staffing costs increased.

5.4. Direct labour costs ($2.519 million)

The NCC anticipates that direct labour costs will amount to $2.519 million in FY 2026-2027. This will support up to 14 full-time equivalents (FTEs) by the completion of FY 2026-2027. This reflects the permanent positions that are proposed in Figure 1 – Organizational Structure of the NCC, Part 4. The administration of the NCC continues to adapt to operational needs, with priority being placed on project delivery and reporting functions.

5.5. Indirect costs – overhead ($0.696 million)

It is anticipated that the NCC's indirect costs will be $0.696 million in FY26/27. Indirect costs include employee benefits, and expenses related to legal advice, insurance, strategic planning processes, and any costs related to the support of the Board of Directors.

5.6. Direct costs ($0.523 million)

The NCC anticipates that the organization's direct costs in FY 2026-2027 will be $0.523 million. Direct costs include expenses related to website development, external audit, the NCC annual conferences, platform construction to support NCC's financial and data management activities, network outreach activities, brand development, and translation services.

5.7. Equipment costs ($0.191 million)

The NCC anticipates that equipment costs in FY 2026-2027 will be $0.191 million. Costs include the acquisition and/or replacement of computers for permanent staff, and allowances for home office equipment. The NCC Board of Directors approved a four-year rotation regarding the replacement of laptop computers for staff in 2025. Also included in this category are licences for software for project management, financial management, and communications activities.

5.8. Subcontractor and consultant costs ($0.149 million)

It is anticipated that the NCC's subcontractor and consultant costs will be $0.149 million for fiscal 2026/2027. Subcontractor and consultant costs will be primarily related to support for hiring and other human resources activities, IT specialists, plus the support of moderators for staff and/or board development activities.

5.9. Travel and outreach costs ($0.099 million)

The NCC's travel and outreach costs are anticipated to be $99,000. Travel and outreach costs will be primarily related to stakeholder engagement and primarily undertaken by the Scientific Director and the Director, Intellectual Property and Partnerships. Travel related to NCC Conferences is considered separately.

Part 6
Risks and Mitigation

Reflecting its commitment to a robust, accountable, and prudent approach to corporate governance, the NCC will regularly identify, assess, and manage any risks related to its objectives and planned activities. As part of its regular operations, the NCC senior team will review and assess all risks.

6.1. Risks and mitigation categories

Organizational risks will be monitored and mitigated according to the four categories described below and in alignment with the planned objectives and activities in this Corporate Plan.

Risk Area	Description
Financial	The risk of financial loss due to the ineffectiveness of financial processes for reporting, budgeting, funding allocation, and fiscal stewardship.
Operational	The risk of direct or indirect loss or inability to provide core services and programs, especially to stakeholders, resulting from inadequate or failed internal processes, legal issues, people, systems, or from external events.
Strategic	The risk associated with changes or impacts to the organization's governance and strategy direction, selection, and execution, or resulting in a lack of achievement of the organization's overall objectives.
Reputational	The risk of loss of reputation and credibility with ecosystem partners, government, and the public. The risk could involve actions or events that create a lasting negative image of, or loss of confidence in, the overall operations of the organization.

6.2. Identified risks and proposed mitigations

Category	Risk	Mitigations
	Further reduction in CSIN contribution agreement funds due to what might appear to be "underspending" on annual / fiscal year request to ISED	• The NCC will ensure improved alignment between funds requested and project expenditures during fiscal years • The NCC will actively seek additional partners for increased research activity • The NCC will increase understanding of the processes involved in grant fund distribution with the government *vis a vis* funding commitments
Financial	Confirming sufficient cash flow for all administrative and project-related requirements.	• The NCC will Improve processes for preparing and submitting requests to ISED for both administrative and grant fund advances • Expansion of NCC financial team and continuous improvement of the NCC's ERP platform to further rationalize internal processes

Category	Risk	Mitigations
	NCC administration costs for salaries, systems, or other overhead could exceed the allocation in the Contribution Agreement funding envelope.	• The NCC will perform ongoing oversight with respect to size and rate of growth of NCC staff complement • The NCC will ensure well-budgeted and well-considered revenue generating activities beyond ISED contributions • The NCC will seek sectoral partners and sponsors to support non-ISED supported activities
	The NCC's 1:1 fund-matching model could pose a risk that partners will be unable to deliver the required matching cash and in-kind contributions set out in the Contribution Agreement.	• The NCC will clearly communicate matching criteria to partners in its Calls for Proposals and communications and will require written acknowledgement from proponents as part of the submission requirements for all Calls for Proposals • The NCC will require documentation from Ultimate Recipients confirming involvement of Participating Organizations through the development of Ultimate Recipient Agreements (URA) before advancing funding

Category	Risk	Mitigations
Program and Operations	The organization could experience delays in implementing systems, processes, and procedures, which could impact timelines set out in the ISED Contribution Agreement and the implementation of organizational activities.	• The NCC may engage external technical expertise to support implementation of systems, in a cost-effective manner • The NCC will continuously monitor and assess progress of operations, and adjust to match capacity
	Given cybersecurity sector labour challenges, the inability to recruit and retain highly skilled and well-established staff in a timely and effective way could pose a risk to operational delivery.	• The NCC will develop a robust and compelling recruitment strategy and process • The NCC will leverage the cybersecurity expertise and their networks to identify potential candidates • The NCC will develop a competitive compensation plan aligned with benchmarks in the finance, IT, and cybersecurity industries

Category	Risk	Mitigations
	The success of the Calls for Proposals could be affected by ill-considered timelines, dissatisfaction of applicants, low-quality proposals, lack of available funds, *etc*.	• The NCC has adapted its Call for Proposals processes significantly with the goal of streamlining and minimizing the work required by applicants, so their time investment scales with their likelihood of success • The NCC will continuously develop and update clear communications and application processes and materials that provide straightforward guidance and clarity on the application process and requirements • The NCC will actively seek grant funds for distribution from other sources, both internal and external to the federal government

Category	Risk	Mitigations
Governance & Strategy	The NCC could confront challenges establishing and retaining a Board with no conflicts of interest, and that reflects its commitments to regional diversity, EDI, and Official Languages.	• The NCC will expand its Board incrementally to ensure that sufficient expertise and diversity is included in its membership • Board Conflict of Interest and Code of Conduct policies are in place and appropriate onboarding processes will ensure that all Board members understand their importance • The NCC Board and senior team will implement a clear process to monitor and manage potential conflicts of interest • The NCC will review and update its Board skills and diversity matrix that reflects its commitments to regional diversity, EDI, and Official Languages. It will proactively address potential bias in its Board construction
	The long-term sustainability of the organization could be threatened if the NCC is unable to create robust and reliable future revenue streams to support operations.	• The NCC will pursue its strategies as defined in its Sustainability Plan as part of its requirements under the Contribution Agreement with ISED • The NCC will continue to pursue a stakeholder / revenue strategy with a focus on ever-increasing value propositions with a clear, revenue-positive fee structure

Category	Risk	Mitigations
Reputational	Perceptions of conflicts of interest could affect the NCC's reputation.	• The NCC will make available its conflict-of-interest guidelines for Board members and team members • The NCC will generally adopt and follow a philosophy of proactive, open, and transparent communications
	Member or ecosystem dissatisfaction with the NCC in relation to operational progress, programs, funding, value creation for members, *etc*., could negatively impact the perceived success of the organization.	• The NCC will continue regular stakeholder communications and outreach Communications will focus on clear and targeted messaging related to NCC Calls for Proposals and activities • With primary support from the Scientific Director, the Director of Intellectual Property and Partnerships, the Board of Directors and SEAC, the NCC will hold ongoing dialogue with members of the Canadian cybersecurity ecosystem, with a commitment to continuous improvement. • The Scientific & Ecosystem Advisory Committee (SEAC) will be expanded to ensure the NCC is well informed about changes appearing across the ecosystem

Category	Risk	Mitigations
	Cybersecurity issues or breaches within the NCC or its partners (e.g., founder institutions, funding partners or Ultimate Recipients of NCC funds) could pose a major reputational risk to the organization.	• The NCC has instituted a Cybersecurity Plan that outlines cybersecurity expectations and requirements for the NCC and Ultimate Funding Recipients • Proof of robust cybersecurity plans are required before funding is awarded to Ultimate Recipients
	Failure to meet Key Performance Indicators (KPIs) as per the requirements of the Contribution Agreement could jeopardize ISED funding.	• The NCC will implement quarterly, semi-annual and annual reporting requirements to the NCC Board with clear guidance for Ultimate Recipients • The NCC will regularly engage with Ultimate Recipients to identify and proactively address emerging concerns with KPIs

Part 7
Performance Management Monitoring Activities

The NCC's performance monitoring strategy outlines the process that the NCC will use to collect, track, and report on the key performance indicators (KPIs) set out in the Contribution Agreement with ISED.

7.1. Reporting roles and responsibilities

Within the NCC, the Director of Programs will work with the Executive Director, the Manager, Communications and the Manager, Finance to oversee the collection, monitoring, and reporting of KPIs. This group, in association with the Scientific

Director, was responsible for setting KPI baselines and targets and confirming the scope and baselines with ISED.

Most of the NCC's established KPIs require timely, accurate reporting from the Ultimate Recipients of NCC funds. The NCC has established a process by which Ultimate Recipients will report quarterly on project activity. The NCC will provide clear guidance to Ultimate Recipients to help to ensure that these reporting requirements are met.

7.2. Reporting mechanisms

The table below describes the NCC's mechanisms to collect, monitor, and report on its KPIs.

Reporting mechanism	Description
Project Reports	In a given fiscal year, Ultimate Recipients will submit project reports quarterly on their projects, including providing data that will contribute to NCC KPIs.
Annual Report	Manager, Communications will oversee the collection of engagement KPIs while the Director of Programs will compile KPI data from Ultimate Recipients' project reports and will submit their findings to ISED as part of the NCC's Annual Report.
Management Review	If deemed necessary, ISED may conduct a management review of the NCC. ISED could ask for an update on KPIs as part of this review.
Final Progress Report	Within 90 calendar days of the Contribution Agreement completion date, the NCC must provide ISED with a final report on how the NCC has achieved its KPI targets.
Post-Contribution Reporting in the Form of an Annual Report	Once the completion date of the NCC Contribution Agreement is reached, the NCC will continue to provide post-contribution reporting for a five-year period, including any updates on achievement of its KPIs in the form of an Annual Report to ISED.

7.3. KPI reporting schedule for 2026-2027

The table below provides a schedule for the NCC to collect, monitor and report on KPIs in 2026-27.

KPI Mechanism	Preparation Time Frame	Deadline
Submission of Project Reports from Ultimate Recipients	Reports with KPIs are submitted quarterly on a rolling basis.	Aggregated by July 31, 2026
Submission of Annual Report	Mid-May to mid-July 2026	July 31, 2026
Submission of Corporate Plan	November 2025 to January 2026	January 31, 2026

List of Appendices

Appendix A – NCC Board of Directors (as of January 31, 2026)

Dr. Charmaine B. Dean, Chair
Vice President, Research and International
University of Waterloo

Mr. Amir Belkhelladi
Partner and National Cyber Leader
Deloitte Canada

Dr. Tim Evans
Vice-President, Research and Graduate Studies
Université Concordia University

Dr. William Ghali
Vice President, Research
University of Calgary

Mr. Antoine Guilman
Co-Leader, Cybersecurity & Data Protection
Gowling WLG

Ms. Elaine Hum
Director, Cybersecurity Partnerships
Scotiabank

Dr. Emily Laidlaw
Canada Research Chair in Cybersecurity Law and Associate Professor
University of Calgary

Dr. Steven Liss
Vice President, Research and Innovation
Toronto Metropolitan University

Dr. David MaGee
Vice President, Research
University of New Brunswick

Mr. Leon Morris
IT Projects Manager, JEDI
Collège Communautaire du Nouveau-Brunswick

Mr. Greg Murray
Sr Vice-President Cybersecurity, Networks, & Technology Risk
Loblaw Companies Ltd

Ms. Olivera Zatezalo
CISO & Vice-President, Cyber IT & Security
Ontario Power Generation

Appendix B - Projected 2026-27 Statement of Operations

REVENUE		
ISED Contribution - Network Activities	$	16 826 109
ISED Contribution - Network Administration	$	3 249 607
Membership Contribution - Network Administration	$	910 813
Other (Sponsorships)	$	150 000
TOTAL REVENUE	$	21 136 529
EXPENSES		
Network Activ ities		
Project Costs	$	16 866 102
Total Network Activities	$	16 866 101
Network Administration		
Payroll & Benefits	$	2 518 488
Training & Development	$	60 000
Equipment & Software	$	190 700
Subcontractors	$	148 500
Travel & Outreach	$	272 000
Insurance	$	25 000
Conference Costs / Event Costs	$	523 000
Total Network Administration	$	3 737 688
TOTAL EXPENSES	$	20 603 789
EXCESS OF REVENUE OVER EXPENSES	$	532 740