National Cybersecurity Consortium

Annual Report - 2022/23

Submitted to Innovation, Science and Economic Development Canada
July 31, 2023

Table of Contents

Message from the Chair

Fiscal year 2022-23 was a critical year for the National Cybersecurity Consortium (NCC). Launching a new organization is always a challenging task, but it was one that its interim Board and Start-up Team embraced with great enthusiasm. Our primary focus was on building the strong foundations that the organization would need to ensure its success now and in the future.

Key achievements included:

1. Establishment of the NCC's basic administrative foundations.
2. Confirmation of the NCC's governance and organizational model.
3. Development of a plan and materials to launch the inaugural call for proposals.
4. Development and completion of a number of the requirements in the Contribution Agreement with ISED.

It takes a village to launch an organization and the NCC was no exception to this rule. In recognition of the many village members who helped to make the NCC's first year a success, I would like to thank a number of people who put their shoulder to the wheel to support the start-up of this organization: my fellow Board members William Ghali (University of Calgary), Charmaine Dean (University of Waterloo), Steven Liss (Metropolitan Toronto University), and David MaGee (University of New Brunswick); our five founders Ken Barker (University of Calgary), N. Asokan (University of Waterloo), Charles Finlay (Metropolitan Toronto University), Mourad Debbabi (Concordia Universiy), and Ali Ghorbani (University of New Brunswick); our government partners at Industry, Science, and Economic Development (ISED), Sinead Tuite, Holly McCracken, and Hamza Khan; and the members of the NCC Start-up Team.

Thank you for the strength of our commitment, passion, and effort. The organization will be stronger because of our work.

As I look back over all that has been accomplished this past year, I feel both confident and excited about the NCC's future. I believe strongly that it will play an essential leadership role within Canada's cybersecurity ecosystem, driving world-class cybersecurity innovation and talent development that will generate and increase cybersecurity-related economic activity in Canada.

Paula Wood-Adams
NCC Chair 2022-23

Introduction

The need for talent development, innovation, commercialization, and collaboration across Canada's cybersecurity ecosystem continues to grow. The increasing adoption of new technologies like artificial intelligence, the Internet of Things, and the worldwide surge in remote and hybrid work has created new and emerging threats to Canada's critical infrastructure, particularly within sectors like energy and utilities, financial services, transportation, and health care. It has also created threats to Canada's open and collaborative research environment.

It is an exciting time, but also one that requires creative thinking, innovative responses, and collaborative approaches. Cybersecurity solutions, products, services, and expertise must keep pace with Canada's digital transformation. This will require significant expansion of shared effort and investment in research, innovation, commercialization, and training across private and public sectors over the next decade. The NCC has been established to help address these needs and we believe that it is well-positioned to provide the leadership that Canada's cybersecurity ecosystem needs to keep Canadians safe.

This Annual Report provides an overview of the critical work undertaken by the NCC in 2022-23, its inaugural year of operations.

About the National Cybersecurity Consortium

The National Cybersecurity Consortium (NCC) is a federally incorporated not-for-profit organization committed to the advancement of Canada's cybersecurity ecosystem. The organization was founded in 2020 by centres of cybersecurity expertise at five Canadian universities: Concordia University, Toronto Metropolitan University, University of Calgary, University of New Brunswick, and University of Waterloo. In February 2022, Innovation, Science, and Economic Development (ISED) committed funding to the NCC over four years 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 industry-academic collaboration.

Our vision: The NCC's vision is to advance Canada's cybersecurity ecosystem through research and development, commercialization, and training.

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.

What we stand for

- **Growth** | We will build innovative cybersecurity systems to establish economic growth and sustainability for Canada and Canadians.
- **Human Resources Skilled in Cybersecurity** | We will develop and offer training programs that meet the true cybersecurity needs of the private and public sectors.

- **Inclusion** | We will integrate the principles of equity, diversity, and inclusion across all areas of the NCC's operations and promote an inclusive organizational culture that values diverse perspectives and contributions.
- **Knowledge Sharing** | We will create a knowledge-sharing community in which access to expertise is available anytime, anywhere from experts and peers.
- **Partnership** | We will promote and cultivate collaboration and partnership opportunities between academia and the private and public sectors.
- **Research and Innovation** | We will build and sustain robust research and development partnerships with industry.

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.

Our Focus

The NCC takes a cross-sectoral approach, cultivating collaboration and capacity-building in the private and public sectors to create economic and social benefits for all Canadians. We catalyze cybersecurity innovation and talent across five areas of focus:

- **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 cyberattacks.
- **Human-centric cybersecurity**: to understand how human factors influence and impact security and privacy requirements to develop new human-centric cybersecurity solutions.
- **Network security**: to develop tools, techniques, and procedures to safeguard computer networks and hosts from both internal and external exploits.
- **Privacy and privacy-enhancing technologies**: to develop protective technologies across many different environments that safeguard individuals and data from privacy violations.
- **Software security**: to develop tools, methods, and practices to reveal and cure vulnerabilities before software is released to end-users.

Launching the National Cybersecurity Consortium

One of the first tasks for the inaugural NCC Board and start-up team was to define the NCC's start-up work plan, which we divided into three phases:

- **Phase One – Building the Foundations (September 2022 - March 2023)**: this phase focuses on establishing the critical operational elements required to deliver on the NCC's vision, mission, and programs.
- **Phase Two – Activation (April 2023 - March 2024)**: this phase builds on the core elements in Phase One to support the activation of key NCC program activities and ecosystem engagement.

- **Phase Three – Full Operations (April 2024 - March 2025**): this phase solidifies administrative and program operations and establishes NCC leadership in the ecosystem.

From September 2022, the interim NCC Board was focused on Phase One – Building the Foundations. The critical work undertaken in this period resulted in the development of strong administrative and governance foundations that will support the successful delivery of programs in 2023 and beyond. In this work, the Board took a measured approach, prioritizing its activities and effectively aligning resources to build organizational success and sustainability.

Critical Achievements - Phase One

The 2022-23 fiscal year was the first year of operations for the NCC. It was a memorable year for this start-up organization that saw the establishment of the critical governance and operational elements that will be required to deliver on our mission, vision, and programs.

The NCC's critical achievements in 2022-23 are highlighted below. They are divided into four key areas of activity: Governance; Administration; Programming; and Communications and Outreach.

Governance

The Board believes that strong governance is essential to building a resilient, effective, and sustainable organization. An essential element of their work this year was investing in building strong governance foundations for the NCC. A key aspect of this work was ensuring that appropriate authorities, accountabilities, and decision-making structures were established. This included developing a governance framework and Board skills matrix to support the creation of a highly qualified, inclusive, 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 were also a central focus of the Board's work. These commitments were concretized in the organization's Corporate Plan, which outlined a clear and strategic plan for its operations in 2023-24, a risk framework that articulates both risks and mitigation strategies, and a monitoring and performance management monitoring activities.

Demonstrating a strong commitment to Equity, Diversity, and Inclusion (EDI), as well as Official Languages, was another priority for the Board in its first year of activity. This commitment shaped the development of both an EDI and an Official Languages Policy that will support the NCC as it strives to integrate its commitments in these areas into all aspects of its work.

Critical Governance Achievements in 2022-23

- Interim Board established
- Governance framework developed
- Board structure confirmed and key committees established
- Key board policies drafted
- First Corporate Plan (2023/24) developed and submitted to ISED
- Official Languages and Equity, Diversity, and Inclusion Policies developed

Administration

Organizations that are successful in delivering on their missions are supported by strong administrative structures and processes. One of the biggest challenges and most critical jobs in any start-up is putting in place these foundational footings and ensuring that they are laid with future resilience and strength in mind.

In September 2022, the Board of Directors appointed a Start-up Lead, who formed a Start-up Team composed of human resources, finance, communications, and policy analysis experts, who were tasked with building the organization's administrative foundations. In collaboration with the Board, this Start-up Team developed key operational policies, including the Employee Code of Conduct and the Employee Conflict of Interest Policy; presented to and received Board approval of HR terms and conditions (e.g., probational period, vacation, hours of work etc..); and analyzed options and provided recommendations to the Board on system (i.e., payroll, benefits, and procurement) implementation and integration with the CRM.

Critical financial processes and procedures were also established. This work included putting in place interim delegated authorities; implementing the NCC banking system and procedures; and appointing a public accountant to audit the NCC's inaugural financial statements.

Critical Administrative Achievements in 2022-23

- Start-up team hired
- Interim Scientific Director appointed and search for Executive Director begun
- Recommendations on system (i.e., payroll, benefits, and procurement) implementation and integration with CRM provided to the Board
- Initial financial processes in place, interim delegated authorities established, and NCC banking system and procedures implemented
- Public accountant appointed to audit the NCC's inaugural financial statements
- Key operational policies drafted and approved, including an Employee Code of Conduct and Conflict of Interest Policy, Travel, and Hospitality Policies
- HR terms and conditions (e.g., probational period, vacation, hours of work etc..) recommended to and approved by the Board

Programming

In its first few years of operation, the NCC's primary activity will be delivering on its commitments to ISED in relation to issuing and managing a series of calls for proposal for research and development, commercialization, and training projects. The NCC is committed to delivering an open, fair, inclusive, and transparent process for these calls.

In support of this commitment, the NCC's interim Scientific Director led the development and design of a critical path for the first call for proposals for implementation-ready projects that included articulation of a rigorous proposal review and ranking process by expert panels and development of a clear application process. He also oversaw development of key guidelines, templates, a project review guide; and communication materials to provide applicants with straightforward guidance on the process and its requirements.

Critical Programming Achievements 2022-23

- Critical path and design of the first call for proposals developed
- Proposal review and ranking process confirmed
- Design of selection and external review committees developed and approved by the Board
- Cybersecurity plan and guidelines drafted
- Key documents, guidance, and communications materials drafted

Communications and Outreach

From its inception, strengthening collaboration and connections across the cybersecurity ecosystem has been central to the vision of the NCC. Building a strong NCC presence and brand is an essential ingredient to success in this area.

One of the first priorities of the Start-up Team was to work on the development of the organization's online presence. As part of this work, an interim brand was developed, including a logo, distinctive colour palette, and administrative templates. The organization's social media channels, namely Twitter and LinkedIn, were also created. In addition, the NCC's bilingual website was developed and launched. These critical pieces of online infrastructure were essential to the promotion of the NCC's first call for proposals and to recruitment of its inaugural Executive Director and team.

Critical Communications and Outreach Achievements in 2022-23

- Online presence confirmed
- Twitter and LinkedIn accounts created
- Bilingual website launched
- Interim branding created
- Interim communications plan drafted

Financial Statements

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Financial Statements
For the year ended 31 mars 2023

Contents

Tél./Tel: 613-237-9331
Téléc./Fax: 613-237-9779
www.bdo.ca

BDO Canada s.r.l./S.E.N.C.R.L./LLP
180 Kent Street
Suite 1700
Ottawa ON K1P 0B6 Canada

Independent Auditor's Report

To the members of
National Cybersecurity Consortium

Opinion

We have audited the accompanying financial statements of National Cybersecurity Consortium (the "Consortium"), which comprise the statement of financial position as at March 31 2023, and the statements of operations, changes in net assets and cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In our opinion, the accompanying financial statements present fairly, in all material respects, the financial position of the Consortium as at March 31 2023, and its results of operations and its cash flows for the year then ended in accordance with Canadian accounting standards for not-for-profit organizations ("ASNPO").

Basis for Opinion

We conducted our audit in accordance with Canadian generally accepted auditing standards. Our responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of our report. We are independent of the Consortium in accordance with the ethical requirements that are relevant to our audit of the financial statements in Canada, and we have fulfilled our other ethical responsibilities in accordance with these requirements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Emphasis of Matter

We draw attention to Note 2 of the financial statements which describes that the Consortium adopted Canadian accounting standards for not-for-profit organizations on April 1, 2022 with a transition date of April 1, 2021. These standards were applied retrospectively by management to the comparative information in these financial statements, including the statement of financial position as at March 31, 2022, and the statement of change in net assets, statement of operations, and statement of cash flow for the year ended March 31, 2022, and related disclosures. We were not engaged to report on the restated comparative information, and as such, it is unaudited.

Responsibilities of Management and Those Charged with Governance for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with ASNPO, and for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is responsible for assessing the Consortium's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless management either intends to liquidate the Consortium or to cease operations, or has no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the Consortium's financial reporting process.

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with Canadian generally accepted auditing standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with Canadian generally accepted auditing standards, we exercise professional judgment and maintain professional skepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Consortium's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.

- Conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Consortium's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Consortium to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

BDO Canada LLP

Chartered Professional Accountants, Licensed Public Accountants
Ottawa, Ontario
July 5, 2023

National Cybersecurity Consortium
Statement of Financial Position

March 31	2023	2022
		(unaudited)
Assets		
Current		
Cash	**$ 501,089**	$ 57,601
Harmonized sales tax receivable	**23,778**	-
Prepaid expenses	**10,515**	-
Total Assets	**$ 535,382**	$ 57,601
Liabilities and Net Assets		
Current		
Accounts payable and accrued liabilities	**$ 164,346**	$ -
Deferred contributions (Note 4)	**200,719**	-
Due to related party (Note 3)	**150,000**	-
	515,065	-
Net Assets		
Unrestricted	**20,317**	57,601
Total Liabilities and Net Assets	**$ 535,382**	$ 57,601

On behalf of the Board:

_____ Director _____ Director

The notes are an integral part of these financial statements.

National Cybersecurity Consortium
Statement of Changes in Net Assets

For the year ended March 31	2023	2022
		(unaudited)
Balance, beginning of the year	**$ 57,601**	$ -
Excess (deficiency) of revenues over expenses	**(37,284)**	57,601
Balance, end of the year	**$ 20,317**	$ 57,601

The notes are an integral part of these financial statements.

National Cybersecurity Consortium
Statement of Operations

For the year ended March 31 2023	2023	2022
		(unaudited)
Revenues		
Contributions from ISED	**$ 544,048**	$ -
Contributions from founding members	**-**	150,000
ISED expenses		
Direct costs	**2,885**	-
Direct labour	**103,657**	-
Indirect costs	**81,379**	-
Sub-contracting	**380,494**	
Total ISED expenses	**568,415**	-
Inegible expenses	**12,917**	92,399
Total expenses	**581,332**	92,399
Excess (deficiency) of revenues over expenses	**$ (37,284)**	$ 57,601

The notes are an integral part of these financial statements.

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Statement of Cash Flows

For the year ended March 31 2023	2023	2022
		(unaudited)
Cash flows from operating activities		
Excess (deficiency) of revenues over expenses	**$ (37,284)**	$ 57,601
Changes in non-cash working capital:		
Trade and other receivables	**(23,778)**	-
Prepaid expenses	**(10,515)**	-
Accounts payable and accrued liabilities	**164,346**	-
Deferred contributions	**200,719**	-
	293,488	57,601
Cash flows from financing activities		
Advance from related party	**150,000**	-
Net increase in cash	**443,488**	57,601
Cash, beginning of the year	**57,601**	-
Cash, end of the year	**$ 501,089**	$ 57,601

The notes are an integral part of these financial statements.

31 mars 2023

1. Accounting Policies

Purpose of Consortium

National Cybersecurity Consortium (the "Consortium") is a not-for-profit organization incorporated without share capital under the Canada Not-for-profit Corporations Act on March 3, 2020, as a member-based organization with an agreement between Innovation, Science and Economic Development Canada (ISED) and the National Cybersecurity Consortium. The Consortium qualifies as a non-profit organization as defined in the Income Tax Act and, as such, is exempt from income tax.

The Consortium's mandate is to advance Canada's cybersecurity ecosystem through research and development, commercialization, and training.

Basis of Accounting

The Consortium applies the Canadian accounting standards for not-for-profit organizations ("ASNPO").

Revenue Recognition

The Consortium follows the deferral method of accounting for contributions. Restricted contributions are recognized as revenue in the year in which the related expenses are incurred. Unrestricted contributions are recognized as revenue when they are received or receivable if the amount to be received can be reasonably estimated and collection is reasonably assured.

Financial Instruments

Initial and subsequent measurement
The Consortium initially measures its financial assets and liabilities at fair value. The Consortium subsequently measures all its financial assets and financial liabilities at amortized cost.

Impairment
Financial assets measured at amortized cost are tested for impairment when there are indications of possible impairment.

Transaction costs
Transaction costs related to financial instruments subsequently measured at amortized cost are included in the original cost of the asset or liability and recognized in the statement of operations over the life of the instrument using the straight-line method.

2. First-time Adoption of Accounting Standards for Not-for-Profit Organizations

Effective April 1, 2021, the Consortium adopted the requirements of the new accounting framework: Canadian accounting standards for not-for-profit organizations (ASNPO) or Part III of the requirements of the CPA Canada Handbook – Accounting. These are the Consortium's first financial statements prepared in accordance with this framework. First-time adoption of this basis of accounting had no impact on the Consortium's excess of revenues over expenses for the year ended March 31, 2022, or on net assets as at April 1, 2021, the date of transition. An opening statement of financial position at the date of transition has not been presented, given the Consortium had no activity prior to July 21, 2021.

3. Due to Related Party and Related Party Transactions

The Consortium has five founding members - University of Waterloo, University of New Brunswick, Toronto Metropolitan University, University of Calgary and Concordia University.

During the year, the Consortium received financing of $150,000 through promissory note from one of the founding members. The promissory note carries no interest and is payable by April 30, 2023.

4. Deferred Contributions

The Consortium received and used funding from ISED as follows :

	2023	2022
Balance, beginning of year	**$ -**	$ -
Plus: Contributions received in the current year	**744,767**	-
Less: Recognized as revenue in the year	**(544,048)**	-
Balance, end of year	**$ 200,719**	$ -

5. Financial Instruments

Liquidity risk
The Consortium is exposed to the liquidity risk mainly in respect of accounts payable, accrued liabilities, deferred contributions and the promissory note due to a related party.

Credit risk
The Consortium's is also exposed to the credit risk arising from all of its bank accounts held at a single financial institution.