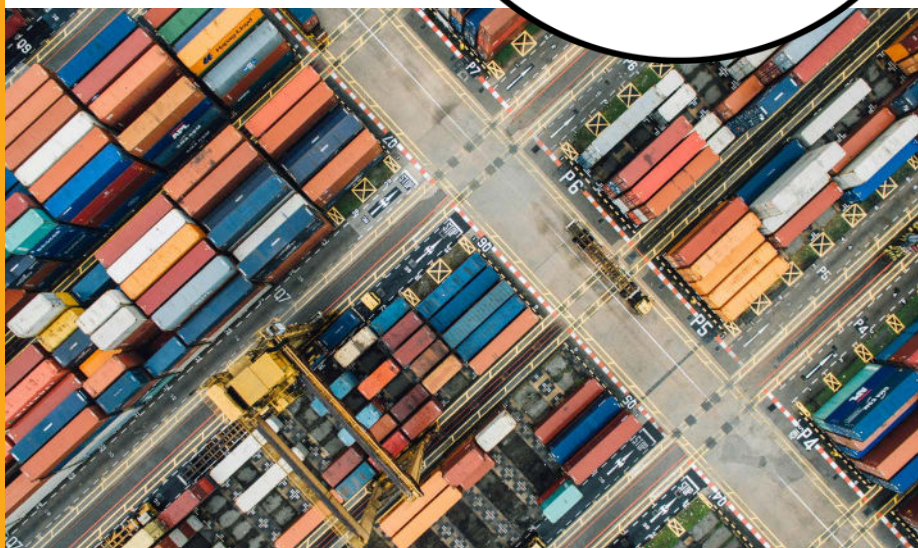




2025 - 2026 Annual Report



Building Canadian
Digital Sovereignty Through
**Collaboration,
Innovation +
Talent Development**

A Message from the Chair of the Board



Dr. Charmaine Dean

As Canada embraces its role as a trusted leader in a new era of technological expansion, developing AI, preparing for quantum and keeping an eye on the horizon for the next challenge, success in these areas will require a strong and sustainable cybersecurity underpinning. The National Cybersecurity Consortium (NCC) has become a critical partner in Canadian cybersecurity development and readiness.

In its three years of operation, the NCC has proven itself to be an effective and vital partner in the support and development of Canada's cybersecurity ecosystem, and a respected steward of Canada's Cyber Security Innovation Network (CSIN). To date, the NCC has committed more than \$55 million in funding to critical cyber research, development, training and commercialization programs across the country.

These investments, as well as the active development of Canada's cybersecurity ecosystem, have been integral in building a framework for sovereign Canadian cyber solutions.

The NCC and its team actively position themselves as one of Canada's most essential and dynamic cybersecurity ecosystem entities. Under the leadership of Scientific Director Ken Barker, the team delivers effective, high-impact programs and has built a pan-Canadian, interconnected network of cybersecurity experts.

I want to thank my fellow NCC Board members, and the entire NCC team for their service to this critical strategic environment. I would also like to thank the Government of Canada, through the Ministries of Industry and Artificial Intelligence and Digital Innovation for their focus on this critical area. Your dedication and creativity have been vital to the NCC's success in this past year, and it has been my honour to work with you.

Sincerely,

Charmaine Dean

NCC Board of Directors

The NCC expanded its Board of Directors to 13 members, including four members recruited from the larger Canadian cybersecurity community in 2025.



Amir Belkhelladi

Partner and National Leader,
Cyber Risk Services, Deloitte



Dr. Tim Evans

VP, Research, Innovation & Impact,
Concordia University



Dr. William Ghali

VP, Research,
University of Calgary



Dr. Antoine Guilmain

Co-Leader Cybersecurity & Data,
Protection, Gowling WLG



Elaine Hum

Director, Cybersecurity Partnerships,
Scotiabank



Marc Kneppers

President & CEO,
Goldenrod Consulting

NCC Board of Directors (cont.)



Dr. Emily Laidlaw

Associate Professor and Canada,
Research Chair in Cybersecurity Law,
Faculty of Law, University of Calgary



Dr. Steven N. Liss

VP, Research and Innovation Toronto,
Metropolitan University



Dr. David MaGee

VP, Research,
University of New Brunswick



Leon "Lee" Morris

IT Projects Manager – Lead Instructor, Joint
Economic Development Initiative, Collège
communautaire du Nouveau-Brunswick



Greg Murray

SVP Cyber Security, Privacy & Network,
Loblaw Companies Ltd.



Olivera Zatezalo

CISO & VP, Cyber and IT Security,
Ontario Power Generation

A Message from the Scientific Director, National Cybersecurity Consortium



Dr. Ken Barker

The NCC has had a very productive year. We have now undertaken three full funding calls and have built key partnerships across the country that continue to impact the Canadian cybersecurity ecosystem.

We have committed \$55 million in funding via 81 distinct projects through the Cyber Security Innovation Network (CSIN). The Canadian cybersecurity community has committed to matching these funds, which will allow us to provide a total impact exceeding \$134 million over the next few years. These projects will continue to support Canada and help protect Canadians.

This year has been a transitional one for the country with major new investments in defence, the development of the Defence Industrial Strategy (DIS) and a significant forward-looking commitment to emerging technologies in artificial intelligence and quantum through the establishment of the Ministry of Artificial Intelligence and Digital Innovation (AIDI). The DIS will require further cybersecurity investment to both protect Canadian defence infrastructure when troops are deployed or protecting the Arctic as we move to better protect our national sovereignty, and lead globally in key areas of cyber that are capable of disrupting those who would threaten Canada. The NCC's stakeholder community is well positioned to assist in this critical area of our national security.

Artificial intelligence is emerging as an existential threat to our public and private sector organizations with the development of Frontier AI and advanced LLMs capable of identifying vulnerabilities in systems that were previously unknown. This has always been a challenge in cybersecurity, but what has changed is the speed at which vulnerabilities can be discovered and the requirement to respond to them more expeditiously to protect critical infrastructure and supply chains. Advanced AI will continue to challenge personal privacy, and as advanced frontier models continue to onboard large amounts of data, we will need to find ways to protect Canada and Canadian's digital sovereignty.

The NCC's members and their collaborators from the private and public sector are anxious to expand upon their work to address the challenges from both new priority areas. There are over 140 post-secondaries and more than 200 private and not-for-profit organizations working on NCC funded projects that are keen to take on these new challenges and have the expertise to have an impact very quickly. The NCC is excited about coordinating with these stakeholders in an anticipated Call 2027 that will address these emerging new challenges.

The NCC is very thankful for the strong support received from the federal government, who has ensured that we are meeting our goals, and who has assisted time and again in finding ways to get things done. In addition, I would like to thank the wider community of cyber experts from all sectors for their contributions to the NCC including providing advice, reviews of projects, applications for funding and moral support as we have built up the NCC.

I want to thank our Board for their unwavering commitment to the NCC, its goals and vision and our staff as they continue to work hard to establish a truly visionary approach to meeting a core need for Canada. Your vision, commitment and expertise will allow the NCC to thrive and diversify its value proposition to its members as we move into the third full year of our operations.

Sincerely,

Ken Barker



CALL FOR PROPOSALS IN REVIEW

Cyber Security Innovation Network (CSIN)

Years
Active

2023

2024

2025

86 Funded
Projects

42 Awardees

453 Partner
Organizations

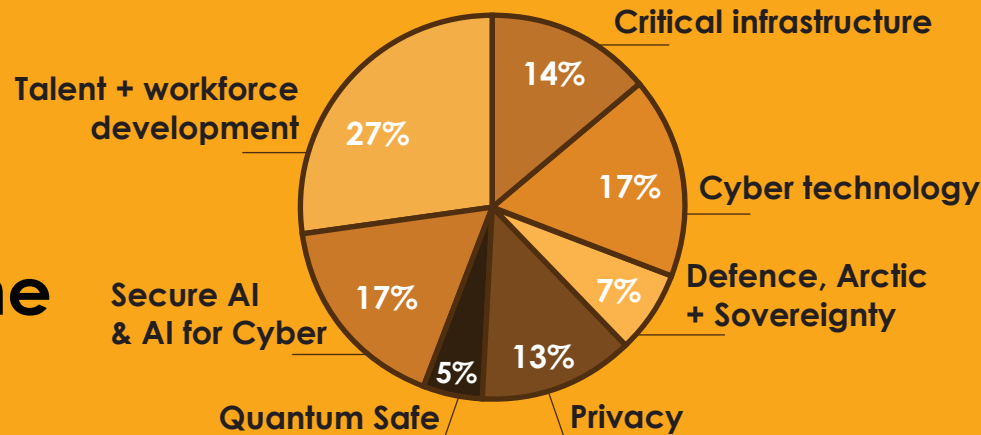


\$53.2 million
Funds Distributed by CSIN



\$79 million
Invested by Collaborators

Funded Projects by Theme



Funded Projects by Stream

63 Research 19 Training 4 Commercialization



Funded Projects by Sector

70 Academic 13 Industry 3 Not-for-profit



Funded Projects & Collaborators

Funded Projects

AB	16
BC	10
MB	0
NB	5
NL	2
NS	2
NT	0
NU	0
ON	34
PE	0
QC	16
SK	1
YK	0

Project Collaborators

AB	70
BC	33
MB	4
NB	18
NL	4
NS	11
NT	0
NU	1
ON	175
PE	0
QC	102
SK	9
YK	1

International 25

2025

Call for Proposals

In 2025, the NCC committed \$20,998,698 in funding 31 new projects, and top-up funds to previously awarded projects from Calls 2023 and 2024. This brings the total investment to over \$135 million in cybersecurity project activities, further mobilizing innovation and supporting upskilling in Canadian cybersecurity across the country.

Securing Canada's Digital Future

The NCC's funding program exists to stimulate a strong national cybersecurity ecosystem and position Canada as a global leader in cybersecurity. Since 2023, the NCC has funded cybersecurity projects in three funding categories: **Commercialization, Research and Development and Training**. These projects represent a diverse range of activity within our five areas of focus: Critical infrastructure protection, human-centric cybersecurity, network security, privacy and privacy-enhancing technologies, and software security.

The NCC used the 2025 Call for Proposals to assess the need in the Canadian cybersecurity ecosystem for the funding of different types of projects. This year's funding call included three categories:

Category 1, Accelerated Projects: Intended to make impactful progress on highly targeted, larger budget projects;

Category 2, New 2025 Projects: An open call for cybersecurity and privacy-related projects; and

Category 3, Top-ups to 2023/2024 Projects: Intended to increase the impact of projects already vetted and approved by the NCC by allowing them to incorporate nascent insights or cover gaps that emerged through the work to date.

Projects were peer-reviewed by over 35 subject matter experts in the Canadian cybersecurity ecosystem across 8 subcommittees and approved by the NCC's Board of Directors.

Future Calls

The NCC and Innovation, Science and Economic Development Canada (ISED) have continued conversations regarding ongoing support for the cybersecurity ecosystem, including a Call in 2027. However, with changes in government priorities, the renewal of the CSIN program remains uncertain.

We are incredibly proud of the achievements made by our funded projects and are dedicated to working toward continued support for future talent and innovation.

Post-Award Monitoring & Support

To support our awardees, information and help sessions are provided quarterly to assist with reporting. We continue to streamline processes and identify efficiencies to meet our obligations to ISED.

2025 Funded Projects

Accelerated Projects

Commercialization

CYBERDEFENSE AI Go-To-Market 2025-2027

Recipient: CYBERDEFENSE AI, Montréal, QC

Collaborators: Cybereco

Committed Funds: \$142,250

Research & Development

Secure Healthcare Data Federation through Generative Access Control

Recipient: Otekha Health Corporation, Kitchener, ON

Collaborators: University of Toronto, University of Calgary, University of Waterloo, University of New Brunswick

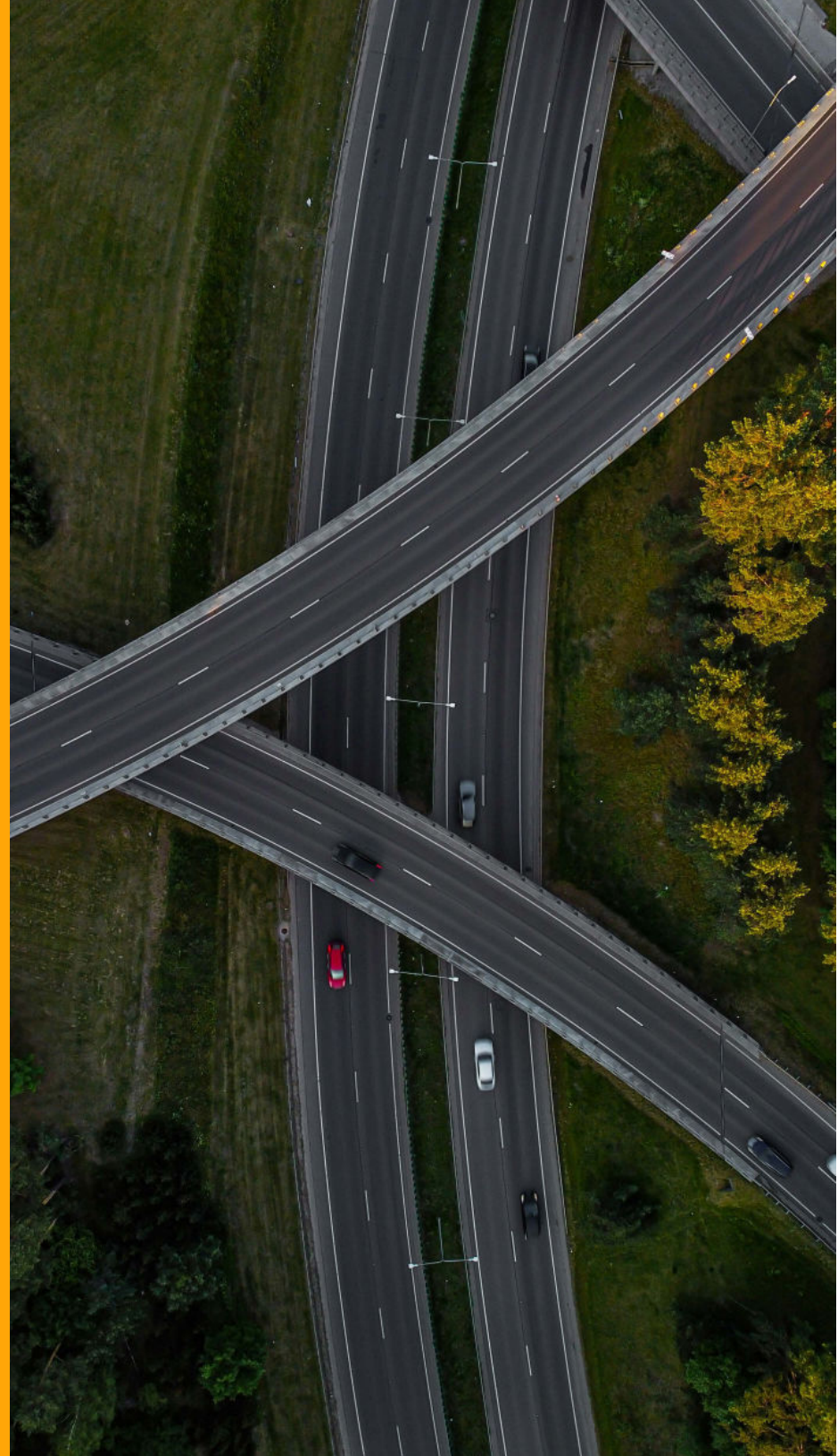
Committed Funds: \$2,384,650

Protecting Alberta & Nunavut HigherEd with Global Partnerships

Recipient: Cybera Inc., Calgary, AB

Collaborators: AARNet, University of Calgary, University of Alberta, Nunavut Arctic College

Committed Funds: \$2,500,000



New Projects

Research & Development - Spearhead

May We Have Your Attention Please? Exploring How Employee Attention Influences Cybersecurity Behaviour

Recipient: University of Waterloo, Waterloo, ON

Collaborators: University of Delaware, TU Darmstadt

Committed Funds: \$223,529

Digital Warrior

Recipient: Humber College, Etobicoke, ON

Collaborators: White Bear Education Complex

Committed Funds: \$482,375

Cyber-Synthetic Risk: A Generative Multi-Agent Approach to Forecasting Advanced Cyberattack Impacts on Enterprise Ecosystems

Recipient: University of Guelph, Guelph, ON

Collaborators: Fortinet Canada, InCloud Security Inc., RiskView Inc, Toronto Community Housing Corporation, University of Toronto, École de technologie supérieure Engineering, University of New Brunswick, Brandon University

Committed Funds: \$159,850

Self-Healing AI Security via Autonomous Patch Generation & LLM Autovaccination

Recipient: University of Guelph, Guelph, ON

Collaborators: 3Tenets Consulting, eSentire Corp, ISACybersecurity Ltd, Wellington-Dufferin-Guelph Public Health, McGill University, University of Saskatchewan, Dalhousie University

Committed Funds: \$182,671



STAY SAFE TEAM

CAF ARC

AI-Driven IoT Threat Intelligence: Securing Smart Environments Across Zigbee, Z-Wave, Bluetooth, and Wi-Fi Networks

Recipient: Dalhousie University, Halifax, NS

Collaborators: York University, Solana Networks

Committed Funds: \$499,100

Differential Programming and Fully-Homomorphic Encryption at the Edge

Recipient: Simon Fraser University, Burnaby, BC

Committed Funds: \$494,115

Securing the Canadian Software Supply Chain

Recipient: University of Calgary, Calgary, AB

Collaborator: BoostSecurity.io

Committed Funds: \$470,588

Securing Agentic AI Systems Across the Development and Operations Lifecycle

Recipient: Polytechnique Montréal, Montréal, QC

Collaborator: University of Waterloo

Committed Funds: \$500,000

Cyber Resilient Battery Management System with secure Bi-directional Power Flow for Connected Vehicles

Recipient: Ontario Tech University, Oshawa, ON

Collaborator: Toronto Metropolitan University

Committed Funds: \$500,000

Vulnerabilities and Defenses of Online Interactive Discussion Forums to Interference by Generative AI

Recipient: University of British Columbia, Vancouver, BC

Committed Funds: \$500,000

Securing LLM Agents Against Malicious or Vulnerable Tools

Recipient: University of Waterloo, Waterloo, ON

Committed Funds: \$254,116

Zero-Knowledge Threat Detection and Risk Assessment in Aerospace and Orbital Infrastructures

Recipient: McGill University, Montréal, QC

Collaborators: CAE Inc, Royal Military College of Canada, Queen's University

Committed Funds: \$500,000

Threat Modelling and Mitigation of Human-factors Based Exploits in Advanced Driver Assistance Systems

Recipient: University of Western Ontario, London, ON

Collaborator: Acerta

Committed Funds: \$481,850

Efficiency and Security of Unknown Group Order Cryptography

Recipient: University of Calgary, Calgary, AB

Collaborator: Pacific Institute for the Mathematical Sciences

Committed Funds: \$499,411

Reliable and Explainable Malware Detection

Recipient: University of British Columbia, Vancouver, BC

Committed Funds: \$262,200

The Location Dragnet

Recipient: University of Calgary, Calgary, AB

Collaborators: York University

Committed Funds: \$450,000

Frontier Quantum-AI Cyber Defense: Pioneering Unprecedented Security Measures for Critical Infrastructure

Recipient: University of Calgary, Calgary, AB

Collaborators: IoTech Lab, Quantum City, Axiom Technology, Dalhousie University, Pauli Group Inc

Committed Funds: \$500,000

Post Quantum Resilience of Cyber-physical Power Systems

Recipient: Toronto Metropolitan University, Toronto, ON

Collaborators: ABB Canada, Hydro Québec – IREQ

Committed Funds: \$500,000

Research & Development - Standard

Cybersecurity, Resilience, and Trustworthiness of Networked Critical Infrastructure and Autonomous Advanced Air Mobility (AAM) Assets Against Malicious Adversary Cyber-attacks

Recipient: Concordia University, Montréal, QC

Collaborators: University of Windsor, University of Alberta, University of Manitoba, VOZWIN Inc., HUMANITAS Inc.

Committed Funds: \$1,997,550

Digital Twin Platform for Critical Infrastructure Cybersecurity Modeling and Assessment

Recipient: British Columbia Institute of Technology, Burnaby, BC

Collaborators: BC Hydro, Siemens Canada, Awesense, Islay Power, EdgeTune Power, Fuse Power, ETECTRIX, Hydron Energy, Kwantlen Polytechnic University

Committed Funds: \$900,000

Prescriptive Analysis & Agentic Solutions for Disinformation & Digital Attacks

Recipient: Koat.ai Incorporated, Calgary, AB

Collaborators: FORESIGHT REPORTS, Alberta Innovates, ALTAML

Committed Funds: \$625,000

MATSEC: Materials-based Cybersecurity in Electronics

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Palitronica, Wade Antenna

Committed Funds: \$2,000,000

Training

Shields Activated – Strengthening Cyber Resilience for Small Businesses

Recipient: Protexxa Inc., Aurora, ON

Collaborators: Ontario Tech University

Committed Funds: \$1,000,000

Critical Infrastructure Cybersecurity Experiential Training Program

Recipient: British Columbia Institute of Technology, Burnaby, BC

Collaborators: BC Hydro, EdgeTune Power Inc., Fortis BC

Committed Funds: \$310,000

A Comprehensive Training Program for Advanced Cybersecurity in 5G Networks, ICS/CPS, and Beyond

Recipient: Concordia University, Montréal, QC

Collaborators: University of Ontario Institute of Tech (UOIT), Ericsson

Committed Funds: \$500,000

Driving Cybersecurity Excellence: Pathways To Reduce Labour and Skills Gaps

Recipient: Digital Nova Scotia, Halifax, NS

Collaborators: University of Waterloo, St. Francis Xavier University, Government of Nova Scotia

Committed Funds: \$498,943

First Response for Cyber Threats (FRCT) - A Collaborative Cybersecurity Training Initiative

Recipient: University of Windsor, Windsor, ON

Collaborators: Sterling Information Technology, WE-Tech Alliance

Committed Funds: \$350,000

Preparing Canada's Workforce for the Future of Cybersecurity through Training and Academic Pathways

Recipient: Concordia University of Edmonton, Edmonton, AB

Committed Funds: \$330,500



Top-up Funds for 2023/2024 Awarded Projects

PASCAL

Recipient: Palitronica, Waterloo, ON

Collaborator: Internal

Committed Funds: \$500,000

Building Cyber Resilient and Secure 5G Networks Through Automation and AI

Recipient: Concordia University, Montréal, QC

Collaborator: Ericsson

Committed Funds: \$500,000

Fortifying Cybersecurity: Early Ransomware Detection & Mitigation Methods

Recipient: University of New Brunswick, Fredericton, NB

Collaborator: Research NB Emerging fund – 2025

Committed Funds: \$25,000



NCC's Inaugural Conference

June 25 - 27, 2025

**Banff Centre for Arts and Creativity
Banff, Alberta**

The NCC's 2025 Conference acted as a hub for Canadian experts and leaders in cybersecurity to convene, exchange ideas, expand professional networks and co-create strategies to elevate the country's cybersecurity ecosystem.

This event was primarily invitation-only, and catered to those leading innovation, senior and emerging researchers and supporters of cutting-edge technology who all share a commitment to advancing the field in Canada. More than 130 participants attended over two days of panels, discussions and workshops. The NCC also hosted, in association with Mastercard, a Capture the Flag competition for post-secondary students studying cybersecurity and other related fields.

NCC Grantees presented posters that featured their cybersecurity and privacy projects. This offered a rich opportunity for attendees to explore new and developing research, training initiatives and commercialization projects happening in Canada. The NCC also hosted a Capture the Flag event for students from Canadian post-secondary institutions.

The NCC has been relatively successful in attracting academic participants to its limited events, as well as those in parallel not-for-profit organizations involved in cybersecurity and privacy issues in Canada. The NCC has been less successful in attracting for-profit entities to participate and support the organization, especially after economic concerns driven by tariff issues by the United States.



2025 CAPTURE THE FLAG

A cybersecurity student event made possible by Mastercard

June 25, 2025, Remote + at the Banff Centre for Arts and Creativity, Banff, AB

The NCC held its first-ever Capture the Flag (CTF) competition made possible by Mastercard and powered by ENFOCOM Cyber. The hybrid event was held at the Banff Centre for Art and Creativity in Banff, AB, with 25 participating teams made up of 78 students in total.

The teams were comprised of students from Canadian post-secondary institutions and competed for top-ranking places and prizes. Three Alberta-based high school teams participated in a non-competitive category and kept up exceptionally well with the post-secondary students in both skill and knowledge.



Mastercard Capture the Flag Series 2026

Presented by the
National Cybersecurity Consortium

In 2026, the NCC and Mastercard teamed up once again, but this time to host a series of CTF events throughout Canada. This series featured in-person and virtual participation options for students enrolled at a Canadian post-secondary institution. The challenges offered a hands-on way to learn about cybersecurity regardless of your skill level.

West Regional

Saturday, January 17, 2026

Teams from: Alberta, British Columbia, Northwest Territories, Saskatchewan, Yukon

East Regional

Saturday, February 28, 2026

Teams from: New Brunswick, Newfoundland and Labrador, Nova Scotia, Prince Edward Island

Central Regional

Saturday, February 7, 2026

Teams from: Manitoba, Nunavut, Ontario, Quebec

National Final

Wednesday, June 17, 2026

Teams from anywhere in Canada may participate

Upcoming Events

Canada's cybersecurity ecosystem is diverse and geographically dispersed, creating challenges in building sufficient critical mass to fully capitalize on research outcomes. The NCC has seen these challenges most clearly in the limited number of commercialization projects funded and the shortage of investment funds available to advance promising projects through technology readiness levels toward commercial-ready states.

Active participation with the NCC and its activities provide an opportunity for stakeholders to contribute to addressing these gaps, strengthen connections across the ecosystem, and help create greater momentum around the commercialization of Canadian cybersecurity and privacy research and innovation. Expanding and engaging our stakeholder base is an important part of building the critical mass needed to advance projects and increase opportunities for research outcomes to progress toward commercialization.



Outreach

The NCC continues to strengthen its communications approach to expand its reach and engagement across Canada's cybersecurity ecosystem. A new website is under development to provide a stronger foundation for sharing the NCC's programs, activities, and impact with stakeholders. The NCC has also transitioned to a Canadian-based email marketing platform for its e-newsletters, supporting compliance with Canadian privacy and anti-spam legislation while keeping subscriber data in Canada. Looking ahead, the NCC plans to establish a presence on the Canadian-based social media platform Gander Social once it launches, further expanding the channels available to connect with stakeholders and share information across the ecosystem.

Intellectual Property & Partnerships Report

The Intellectual Property and Partnership (IP&P) team links the NCC to Canadian cybersecurity activities and key regional, sectoral and institutional stakeholders critical to building Canada's cybersecurity and privacy resilience. Specifically, the work of the IP&P team is to focus on developing and retaining Canadian IP. The IP&P team also conceptualizes and develops capacity building plans that align to the NCC mission in collaboration with the NCC's Scientific Director, the Scientific and Ecosystem Advisory Committee (SEAC), NCC Members and other strategic stakeholders.

A Few of the Key IP&P Achievements in 2025-2026:

- The IP&P team conducted research and outreach at cybersecurity, privacy, and other industry events (e.g. InCyber, CPSC, qConnect, webinars, etc.). The resulting analysis linked IP&P engagement to research, policy, and commercial communities across workshops, conferences, and strategic outreach. This work also contributed to an understanding of how AI and Defence impacts IP, particularly as it relates to emergent systems and dual-use technology.
- One sector example of the IP&P team's efforts is its engagement with the Insurance Bureau of Canada to deepen understanding and collaboration opportunities within cyberinsurance markets, cyber-incident response, SME cyber agility, as well as emerging categories of cyber risk.
- The IP&P team delivered two workshops:
 - A workshop on Accelerating CyberAgility in Canadian SMEs explored gaps in how small and medium-sized enterprises (SMEs) can access, adopt, and benefit from cybersecurity tools and services;
 - A workshop on Risk Capital and Commercialization in Cybersecurity explored how Canada can better validate, fund, and grow cybersecurity ventures (e.g. Validation Frameworks for Deep Tech; Cyber Venture Capacity in Research Environments; Cyber Investment as Regional Economic Strategy).



Scientific & Ecosystem Advisory Committee

Throughout the 2025 – 2026 fiscal year, the NCC expanded the capabilities and strategic role of the Scientific & Ecosystem Advisory Committee (SEAC), strengthening its ability to provide insight into emerging cybersecurity trends, ecosystem challenges and future research directions relevant to Canada. Areas of focus included AI-enabled cybersecurity challenges, cybersecurity and AI systems, digital sovereignty and innovation pathways related to DND / CAF engagement.

SEAC was constituted in 2025 and is composed of cybersecurity and privacy leaders drawn from academia, industry, not-for-profits and government. The committee provides the NCC with grounded advice regarding emerging ecosystem needs, capability gaps, evolving research priorities and areas where Canada may face strategic opportunity or risk internationally. SEAC also supports the NCC in understanding how cybersecurity research,

talent, innovation and operational needs are evolving across sectors. SEAC holds biannual meetings, including at the NCC's annual conference.

SEAC advice increasingly focused on how the NCC can strengthen post-award ecosystem development, improve engagement with operational stakeholders and support more coordinated approaches to national cybersecurity priorities. Particular emphasis was placed on the growing overlap between AI, cybersecurity resilience, national security and digital sovereignty, and how these trends are reshaping Canadian capability needs.

To support these objectives, the NCC expanded the workshop series designed to bring together researchers, practitioners, government and operational stakeholders to surface practical insights, clarify priorities and identify opportunities for action. These workshops are intended to strengthen

SEAC's emerging capabilities by supporting more structured ecosystem engagement and helping translate strategic discussion into actionable guidance.

SEAC continues to act as a strategic guide for the NCC, helping identify high-value collaborations, future funding priorities and opportunities to better align research, talent and innovation with clear value for Canadians. The committee also strengthens linkages between the NCC and key sectors including government, public institutions, national security and law enforcement communities, academia and industry.

The NCC highly values the contribution of SEAC members and will continue expanding the committee's engagement and ecosystem reach over the coming year to maximize its strategic value to both the NCC and the wider Canadian cybersecurity ecosystem.

Equity, Diversity, Inclusion & Accessibility

The NCC believes that its mission and vision are best achieved by drawing on the diverse skills, perspectives, experiences, and backgrounds of those in its ecosystem.

In 2025-2026, the NCC prioritized embedding EDIA principles into many areas of its activity:

- All external communications are provided in both official languages and written in clear, accessible plain language.
- Territorial Acknowledgments are reviewed regularly and developed in consultation with local experts to ensure that local context, perspectives, and considerations are appropriately reflected and respected.
- Panelists and moderators invited to participate at NCC Conferences intentionally include individuals with diverse backgrounds wherever possible.
- The NCC's Capture the Flag student competition is designed with accessibility in mind by building functionality for in-person and remote participation. Future events will also be hybrid with in-person events taking place in diverse regions throughout Canada.

Membership

The NCC is fortunate to have a core group of members that have been part of the NCC from the start, and that the membership complement has grown significantly – to 71 base NCC member organizations in the 2025-26 year. NCC base membership is open to organizations based in Canada that span the academia, private industry and not-for profit sectors.

The NCC is grateful to have a strong membership group. NCC base member organizations help the NCC advance the development of the Canadian cybersecurity ecosystem.

For their continued support, the NCC sends its deep appreciation to all the members from the 2025-26 membership year:

Actua	Institut national de la recherche scientifique	Solsys Corporation
BAAR Technologies Inc.	Koat.ai Incorporated	Southern Alberta Institute of Technology
British Columbia Institute of Technology	Lambton College	The Alacrity Foundation of B.C.
Carleton University	Magnificus Software Inc	Humber College
CharliAI Inc.	Manitoba Research Network	Digital Nova Scotia
Concordia University of Edmonton	McGill University	The University of British Columbia
Concordia University	McMaster University	The University of Western Ontario
Cyber PNM Inc	Memorial University of Newfoundland	Toronto Metropolitan University
Cybera Inc	Mycroft Technologies Inc.	Universite De Sherbrooke
Cyberdefense AI	Otekha Health Corporation	Universite Laval
Cybereco	Palitronica	University of Calgary
Dalhousie University	Portage Cybertech Inc.	University of Guelph
DeepCode	Protexxa Inc.	University of New Brunswick
Deloitte	Quantized Technologies Inc.	University of Ontario Institute of Technology
Digital Moment	Quantum Algorithms Institute	University of Ottawa
École Polytechnique de Montréal	Queen's University	University of Regina, Faculty of Engineering
ENFOCOM International Corporation	Redeemer College	University of Saskatchewan
Envisioning Labs	Réseau d'expertise en éthique de données	University of Waterloo
eQualitie Inc	RESTIV Technology Inc.	University of Windsor
Ericsson Canada Inc.	RISQ	University Quebec Outaouais
ezSec Inc	Royal Military College of Canada	UQAM
Field Effect Software	Sheridan College	West Island College Society of Alberta
Fields Institute	Simon Fraser University	York University
Flare Systems Inc.	Skills for Change	

Finance Update

The 2025-26 fiscal year marked the second year of project implementation under the funding agreement with ISED. The organization is now fully staffed and equipped to manage project delivery. The contribution to administrative functions of the NCC amounted to \$3,161,948. The NCC distributed \$16,909,945 in funding from ISED contributions to signed projects from Call 2023, Call 2024 and Call 2025. All contributions received from ISED in 2025-26 were allocated and spent in the current fiscal.

Membership fees collected during the year totaled \$1,007,486, of which \$834,384 was recognized as revenue.

The NCC undergoes an annual financial audit conducted by an independent auditor, approved annually by the Board of Directors and overseen by the Board's Finance & Audit Committee. The financial audit for 2025-26 was completed in June 2026 by BDO Canada LLP with a clean audit opinion. The audited financial statements are included in Appendix 1.

Furthermore, the NCC fully adhered to all regulatory and statutory filing and payment requirements. Our dedication to transparency and compliance highlights our commitment to upholding the highest standard of accountability and governance.

A low-angle photograph of a construction site featuring several large yellow tower cranes against a clear blue sky. The cranes are made of a lattice of metal beams. One crane in the foreground has 'STRABAG' and 'LIEBHERR' written on its side. At the bottom of the frame, the steel framework of a building under construction is visible. On the far left, there is a solid orange vertical bar.

**The right people, having
the right conversations at
the right time.**





www.ncc-cnc.ca



[Follow us on LinkedIn](#)



[Sign-up for our mailing list](#)

Funded by the
Government
of Canada

Canada

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Financial Statements
For the year ended March 31, 2026

Contents

Independent Auditor's Report	2 - 3
Financial Statements	
Statement of Financial Position	4
Statement of Changes in Net Assets (Deficiency)	5
Statement of Operations	6
Statement of Cash Flows	7
Notes to Financial Statements	8 - 10



Tél./Tel: 613-237-9331
Télec./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, 2026, and the statements of operations, changes in net assets (deficiency) 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, 2026, 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.

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.

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 accounting standards for not-for-profit organizations, 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.

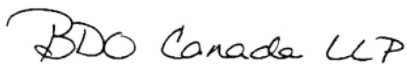
Auditor's Responsibilities for the Audit of the Financial Statements

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.



Chartered Professional Accountants
Ottawa, Ontario
July 28, 2026

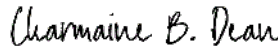
National Cybersecurity Consortium Statement of Financial Position

March 31	2026	2025
Assets		
Current		
Cash	\$ 1,603,898	\$ 1,516,381
Accounts receivable	543,753	191,492
Other receivables	30,815	76,710
Prepaid expenses	182,813	100,375
Project advances	7,785,647	3,994,276
	<u>\$ 10,146,926</u>	<u>\$ 5,879,234</u>
Liabilities and Net Assets		
Current		
Accounts payable and accrued liabilities (Note 2)	\$ 351,435	\$ 292,149
Grants payable - reimbursements	772,965	1,303,926
Grants payable - ultimate recipients	76,684	952,266
Deferred grants and memberships (Note 3)	8,078,354	2,999,526
Due to founding members	115,000	115,000
	<u>9,394,438</u>	<u>5,662,867</u>
Net Assets		
Unrestricted	<u>752,488</u>	<u>216,367</u>
	<u>\$ 10,146,926</u>	<u>\$ 5,879,234</u>

On behalf of the Board:

Signed by:

 _____ Director
 9C036B809006436...

Signed by:

 _____ Director
 41D0855C03A4474...

**National Cybersecurity Consortium
Statement of Changes in Net Assets (Deficiency)**

For the year ended March 31	2026	2025
Balance , beginning of the year	\$ 216,367	\$ (20,311)
Excess of revenues over expenses	536,121	236,678
Balance , end of the year	\$ 752,488	\$ 216,367

National Cybersecurity Consortium Statement of Operations

For the year ended March 31	2026	2025
Revenues		
Grants (Note 3)	\$ 14,449,040	\$ 5,010,800
Memberships (Note 3)	834,384	309,862
Interest and other income	78,270	24,434
	<u>15,361,694</u>	<u>5,345,096</u>
Expenses		
Programs	11,849,056	2,573,147
Program development, delivery, and administration	2,958,296	2,524,935
Unclaimable HST	18,221	10,336
	<u>14,825,573</u>	<u>5,108,418</u>
Excess of revenues over expenses	\$ 536,121	\$ 236,678

The accompanying 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	2026	2025
Cash flows from operating activities		
Excess of revenues over expenses	\$ 536,121	\$ 236,678
Changes in non-cash working capital:		
Accounts receivable	(352,261)	(117,410)
Other receivables	45,906	46,200
Prepaid expenses	(82,439)	(74,029)
Accounts payable and accrued liabilities	59,276	154,693
Deferred grants and memberships	5,078,828	1,485,534
Project advances	(3,791,371)	(3,994,276)
Grants payable –ultimate recipients	(875,582)	952,266
Grants payable –reimbursements	(530,961)	1,303,926
	87,517	(6,418)
Cash flows from financing activities		
Change in due to founding members	-	2,500
Net increase (decrease) in cash	87,517	(3,918)
Cash, beginning of the year	1,516,381	1,520,299
Cash, end of the year	\$ 1,603,898	\$ 1,516,381

National Cybersecurity Consortium

Consortium national pour la cybersécurité

Notes to Financial Statements

March 31, 2026

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.

Use of Estimates

The preparation of financial statements requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and the reported amounts of revenues and expenses for the year covered.

Revenue Recognition

The Consortium follows the deferral method of accounting for contributions. Restricted grant contributions are recognized as revenue in the year in which the related expenses are incurred. Unrestricted grant 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.

Membership fees are recognized as revenue on a pro rata basis over the fiscal year to which they pertain. Amounts received in advance of the applicable fiscal year are recorded as deferred revenue.

**National Cybersecurity Consortium
Consortium national pour la cybersécurité
Notes to Financial Statements**

March 31, 2026

1. Accounting Policies (continued)

Financial Instrument

Arm's length financial instruments are recorded at fair value at initial recognition.

All other financial instruments are reported at cost or amortized cost less impairment. Transaction costs on the acquisition, sale or issue of financial instruments are expensed for those items measured at fair value and charged to the financial instrument for those measured at amortized cost.

Financial assets are tested for impairment when indicators of impairment exist. When a significant change in the expected timing or amount of the future cash flows of the financial asset is identified, the carrying amount of the financial asset is reduced and the amount of the write-down is recognized in net income. A previously recognized impairment loss may be reversed to the extent of the improvement, provided it is not greater than the amount that would have been reported at the date of the reversal had the impairment not been recognized previously, and the amount of the reversal is recognized in net income.

2. Accounts Payable and Accrued Liabilities

Included in accounts payable and accrued liabilities are government remittances payable of \$33,299 (2025 - \$49,344).

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Notes to Financial Statements

March 31, 2026

3. Deferred Grants and Memberships

	<u>2026</u>	<u>2025</u>
Deferred ISED grants	\$ 7,683,846	\$ 2,740,844
Deferred memberships	394,508	258,682
Balance, end of year	\$ 8,078,354	\$ 2,999,526
	<u>2026</u>	<u>2025</u>
Balance, beginning of year	\$ 2,999,526	\$ 1,513,992
Plus: ISED grants received in the current year	19,392,042	6,438,316
Plus: Memberships received in the current year	970,210	367,880
Less: ISED grants recognized as revenue in the year	(14,449,040)	(5,010,800)
Less: Memberships recognized as revenue in the year	(834,384)	(309,862)
Balance, end of year	\$ 8,078,354	\$ 2,999,526

4. Economic Dependence

The Consortium received 94%(2025 - 94%) of its revenues from ISED. Should this funding not be continued or be unable to be replaced, the Consortium wouldn't be able to continue its operations at the current level.

5. Financial Instruments

Liquidity risk

Liquidity risk is the risk that the Consortium may encounter difficulty in meeting its financial obligations as they come due. This includes the risk that, due to operational liquidity constraints, the Consortium may not have sufficient funds to settle transactions on their due dates, may be forced to sell financial assets at unfavorable prices, or may be unable to recover the full value of financial assets. The Consortium is primarily exposed to liquidity risk through its accounts payable, grants payable and accrued liabilities. This risk has decreased from prior year as the accounts payable, grants payable and accrued liabilities balance has decreased.

Credit risk

The Consortium is exposed to the credit risk arising from all of its bank accounts held at a single financial institution. There have not been any changes in the risk from the prior year.