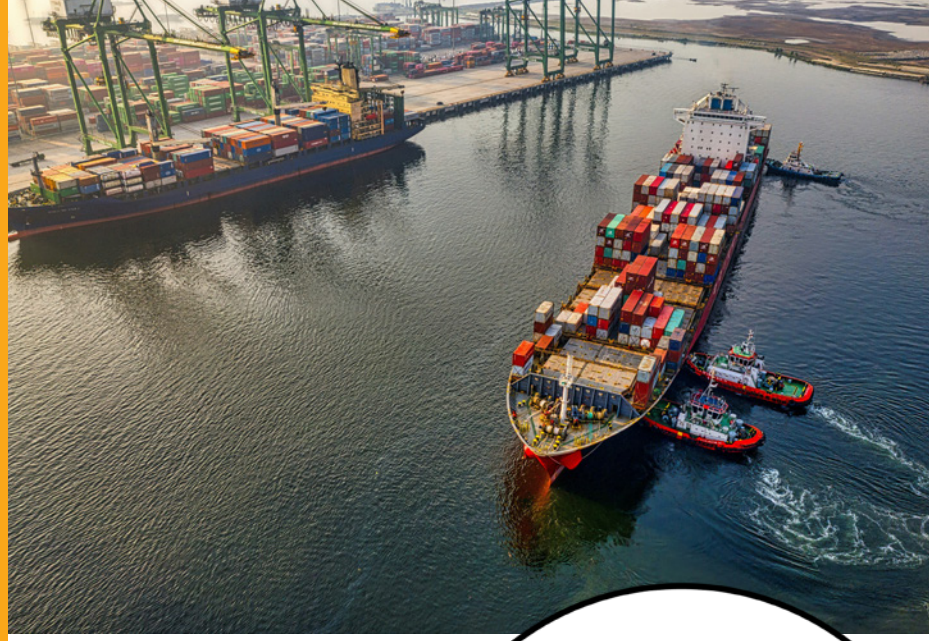


NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

2024 - 2025 Annual Report

A Message from the

Chair of the Board

Dr. Charmaine Dean

Cybersecurity continues to be a critical topic in everyday life in Canada. The National Cybersecurity Consortium (NCC) was created to advance Canada's cybersecurity ecosystem, and to support world class initiatives to keep Canadians safe. Each day, the NCC supports our community and the projects we have funded in our commitment to improve cybersecurity in Canada.

The NCC and the demand for its funding support has grown significantly in our second full year of operation. In 2024, we received more than 90 requests for funding and supported 37 significant Canadian cybersecurity projects with more than $22m in funding. The need for well-funded, far-reaching cybersecurity research, development, training, and commercialization is being well demonstrated.

The NCC and its team have worked diligently to become recognized as one of Canada's most active and vital cybersecurity ecosystem entities. Under the direction of our Scientific Director, Ken Barker, our dedicated team works hard to deliver effective and efficient programs, and to build a pan-Canadian, interconnected membership of cybersecurity experts. Along with our partners at the Cyber Security Innovation Network of the Ministry of Innovation, Science and Economic Development Canada, the NCC has provided a much-needed touch point for the development of programs in cybersecurity across research, educational, and commercialization activities. We see 2024-2025 as a year of further building our community and expanding the scope of our impact for an ever-expanding group of Canadian cybersecurity entities in academia and in the private sector.

I want to thank my fellow NCC Board members, and the entire NCC team for their service to such a game-changing environment. 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

Amir Belkhelladi
Partner and National Leader,
Cyber Risk Services, Deloitte

Dr. Effrosyni Diamantoudi
Dean of Graduate Studies
Concordia University

Dr. William Ghali
Vice President Research
University of Calgary

Elaine Hum
Director, Cybersecurity Partnerships,
Scotiabank

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

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

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

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

A Message from the Scientific Director,

National Cybersecurity Consortium

Dr. Ken Barker

The NCC has had a very exciting and productive year! We have moved from being a "vision" to a "reality" that is impacting the Canadian cybersecurity ecosystem.

This has been our first fully operational year, which included the delivery of first round of funding from the Cybersecurity Security Innovation Network (CSIN) and the roll out of our Call 2024 to identify meritorious cybersecurity/privacy initiatives to support Canada and to help protect Canadians.

The NCC has now put in place a full staff complement to support its activities. The group provides our stakeholders with the highest quality of service to ensure they enable our project leaders to deliver on their goals including training programs, research and development initiatives, and commercialization of innovative ideas. Our team has adopted an internal mantra of "Upholding research … not holding it up!"

We would very much like to thank the many private and public sector participants in the NCC including our cohort of post-secondary stakeholders. In addition, the NCC is very thankful for the strong support received from the federal government, who has helped ensure we are meeting our goals and 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 set 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.

Emerging opportunities around AI and Quantum are being integrated into our thinking about cybersecurity/privacy in Canada in several ways that can be categorized into two dimensions: First, these technologies can be used as tools to enhance security and ensure privacy by using the techniques being developed; and secondly, the threat posed by the emergence and maturation of these technologies present new challenges that need to be addressed as they are deployed. The NCC believes it should take the leadership role in both dimensions by drawing upon our deep expertise in cybersecurity/privacy to ensure that AI/Quantum is applied most effectively to the challenges/opportunities that exist in Canada's digital activities. Significant investments are being made to develop AI and Quantum in Canada, and it is necessary to make corresponding investments in understanding the threats and opportunities they present through the expertise reflected across the NCC. This will ultimately require investment in cyber from public and private sources.

Sincerely,

Ken Barker

2024 Call for Proposals

In our second call for proposals, the NCC committed $21.4 million toward 36 individual projects, which mobilized financial and technical contributions from organizations across Canada. This brings the total project investment in Canadian cybersecurity to over $56 million.

The NCC's annual 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, from building a cyber-resilient secure 5G network using AI, to offering a master's program in cybersecurity.

2024 Funded Projects

Research & Development - Spearhead

Privacy Assurance for Canadian Children: A Safe and Secure Framework for Large Language Models

Recipient: Carleton University, Ottawa, ON

Committed Funds: $88,800

Enterprise-Scale Zero Trust Platform for Privacy-Enhancing Smart Metering Services

Recipient: University of New Brunswick, Fredericton, NB

Committed Funds: $90,390

Securing the Metaverse with Multimodal Access Control and Authentication Methods

Recipient: Institut national de la recherche scientifique, Quebec City, QC

Collaborators: In Virtuo, Beam Me Up, Kaptics, MYND Therapeutics, University of Waterloo, ColAB Numerique, Digital Trust

Committed Funds: $500,000

Enhancing Electric Vehicle Charging Infrastructure Cybersecurity Through Autonomous and Sustainable AI

Recipient: University of Ontario Institute of Technology, Oshawa, ON

Collaborators: University of Western Ontario

Committed Funds: $175,294.10

Ostrich Accounting: Dotting I's and Crossing t's with your Head in the Sand

Recipient: University of Calgary, Calgary, AB

Committed Funds: $500,000

Fully Automated End-to-end Vulnerability Discovery and Repair with LLMs

Recipient: Simon Fraser University, Burnaby, BC

Committed Funds: $500,000

Boosting the Cyber-Resilience of Microgrids within Future Energy Critical Infrastructures

Recipient: Concordia University, Montreal, QC

Collaborators: RMDS Innovation Inc., University of New Brunswick

Committed Funds: $352,940

Adaptive Decision Defense System: A Proactive Approach to Detecting and Mitigating Dual Denial of Decision Attacks in Critical Infrastructure

Recipient: University of Calgary, Calgary, AB

Collaborators: University of Guelph, Laval University, CyberPatterns Inc., Waterfall Security Solutions

Committed Funds: $496,800

ICS Security in the Age of Industry 4.0

Recipient: University of British Columbia, Vancouver, BC

Committed Funds: $500,000

Protecting Democracy from Cyber Threats

Recipient: University of Calgary, Calgary, AB

Committed Funds: $500,000

Preserving Relationship Privacy in Large Networks

Recipient: Simon Fraser University, Burnaby, BC

Committed Funds: $500,000

Novel Methods for Quantifying and Improving Privacy in Machine Learning

Recipient: University of British Columbia, Vancouver, BC

Committed Funds: $495,000

Fortifying Cybersecurity: Early Ransomware Detection and Mitigation Methods

Recipient: University of New Brunswick, Fredericton, NB

Collaborators: University of Ottawa, Bell Canada, EzSec

Committed Funds: $79,500

Combatting Cyber Influence Operations in Online Social Media

Recipient: Université Laval, Quebec City, QC

Collaborators: McGill University, University of Manitoba

Committed Funds: $485,875

Adaptive AI Firewall Specializing in the Protection of AI Models, Critical Infrastructure, Systems, and Agents

Recipient: University of Western Ontario, London, ON

Collaborators: Syngen AI Lab, University of Waterloo

Committed Funds: $500,000

Security Awareness Training through Online Social Learning - "From Phishing through Smishing to Vishing"

Recipient: University of Ottawa, Ottawa, ON

Collaborators: Royal Canadian Mounted Police

Committed Funds: $373,500

Ensuring Mission-Critical Security: Coordination of Autonomous Drone Groups with Security-Aware Decision Making

Recipient: University of Ottawa, Ottawa, ON

Collaborators: Quanser, Concordia University

Committed Funds: $499,100

Cybersecurity assessment of industrial system predeployment models

Recipient: University of Sherbrooke, Sherbrooke, QC

Collaborators: Centris Technologies, Neverhack, Productique Québec

Committed Funds: $480,000

Secure Genomic Data Processing: Unleashing the Potential of Personalized Medicine

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Independent genomics researcher identified

Committed Funds: $129,900

Adaptive Defense Strategies for Advanced Driver-Assistance Systems: A Game-Theoretic Approach

Recipient: University of Waterloo, Waterloo, ON

Committed Funds: $164,622.50

Transformative Adversaries: Leveraging Generative Pretrained Transformers for the Development of Next-Generation Metamorphic Malware Engines

Recipient: University of Ontario Institute of Technology, Oshawa, ON

Committed Funds: $382,352.94

End-to-End Cyber-Security Solution for the Power Grid

Recipient: York University, Toronto, ON

Collaborators: Cistel Technology, Siemens Inc., IESO, Dalhousie University, Carleton University

Committed Funds: $300,000

Research & Development - Standard

Enabling Secure Outsourcing of Sensitive Data

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Amazon AWS, Royal Bank of Canada, Airbus

Committed Funds: $295,000

Authentication for Quantum-Enabled Secure Communication

Recipient: Quantized Technologies Inc., Calgary, AB

Collaborators: University of Calgary

Committed Funds: $940,000

IntruderInsight: Elevating Cyber Attribution with AI Insights

Recipient: ENFOCOM International Corporation, Calgary, AB

Collaborators: University of Calgary – CPSC, Field Effect Software Inc., Raytheon Canada, Cybera, Royal Canadian Mounted Police, Calgary Police Services, Edmonton Police Services, IBM Canada, Université du Québec en Outaouais, Intlabs, Check Point Software Technologies, InceptionU Educational Foundation Ltd., Raytheon Canada, University of New Brunswick, Toronto Metropolitan University – Rogers Cybersecure Catalyst

Committed Funds: $2,000,000

Toward a Secure User-Centric Green Credit Management System

Recipient: University of Calgary, Calgary, AB

Collaborators: Toronto Metropolitan University, University of Alberta, Telus, GuildOne

Committed Funds: $561,000

Revolutionizing Personal Cyber Security with AI-driven Insights

Recipient: Protexxa Inc., Aurora, ON

Collaborators: Toronto Metropolitan University, Core Centre Inc, Mila Montreal

Committed Funds: $1,701,280

SCMS: Securing Critical Marine Systems

Recipient: Memorial University of Newfoundland, St. John's, NL

Collaborators: Dalhousie University, Defense Research and Development Canada Marine Institute, Transport Canada

Committed Funds: $759,073.18

Commercialization

CyberGuardian: Bridging the Cybersecurity Enforcement Training Gap

Recipient: ENFOCOM International Corporation, Calgary, AB

Collaborators: Raytheon Canada, University of Calgary, Royal Canadian Mounted Police, Calgary Police Service, Edmonton Police Service, Check Point Software Technologies, InceptionU Educational Foundation Ltd., University of Ottawa, Field Effect Software Inc., IBM Canada

Committed Funds: $1,000,000

C1R3 Commercialization

Recipient: Portage CyberTech Inc., Gatineau, QC

Collaborators: Converge, Centre for Research and Experimental Development in Informatics Libre, Université de Québec en Outaouais, McGill University, Zu, Flex Groups

Committed Funds: $1,000,000

Training

IncidentSync: Bridging IT and Law Enforcement

Recipient: ENFOCOM International Corporation, Calgary, AB

Collaborators: Field Effect Software Inc., Toronto Metropolitan University - Rogers Cybersecure Catalyst, Royal Canadian Mounted Police, Calgary Police Services, Edmonton Police Services, University of Calgary - Cont. Ed., InceptionU Educational Foundation Ltd., Intlabs, Université du Québec en Outaouais, Savvy Knowledge Corporation, Raytheon Canada, IBM Canada, Check Point Software Technologies

Committed Funds: $1,000,000

Accelerating Efforts to Secure Canada in an Era of Quantum

Recipient: Quantum Algorithms Institute, Surrey, BC

Collaborators: Field Effect, Information and Communications Technology Council, Canadian Information Processing Society, Beauceron Security, Quantum Algorithms Institute, Durham College

Committed Funds: $1,000,000

Human-Centric Immersive Cybersecurity Training: Socio-Technical and Legal Implications of an Attack

Recipient: University of Ottawa, Ottawa, ON

Collaborators: Université de Montréal, University of Calgary, ENFOCOM, Field Effect, IBM, Desjardin, BNC (to be confirmed)

Committed Funds: $961,400

CRAFT: Cybersecure Robotics and Future Talent

Recipient: University of Waterloo, Waterloo, ON

Collaborators: Cobionics, Labforge, Canadian Nuclear Labs, BTQ, Palitronica, Quanser, Alectra, Milton Hydro, Real Life Robotics

Committed Funds: $1,000,000

MCT: Marine Cybersecurity Training

Recipient: Memorial University of Newfoundland, St. John's, NL

Collaborators: Thales

Committed Funds: $1,000,000

Training for proactive interdisciplinary cybersecurity in the workplace

Recipient: University of Sherbrooke, Sherbrooke, QC

Collaborators: Cybereco, Intact corporation financière

Committed Funds: $580,679

2025
Call for Proposals

In our third call for proposals, the NCC will commit over $20 million toward cybersecurity and privacy projects in Canada.

For the 2025 Call for Proposals, the NCC implemented three new categories to accommodate different types of projects within the Canadian cybersecurity and privacy ecosystem. The new funding Categories include:

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

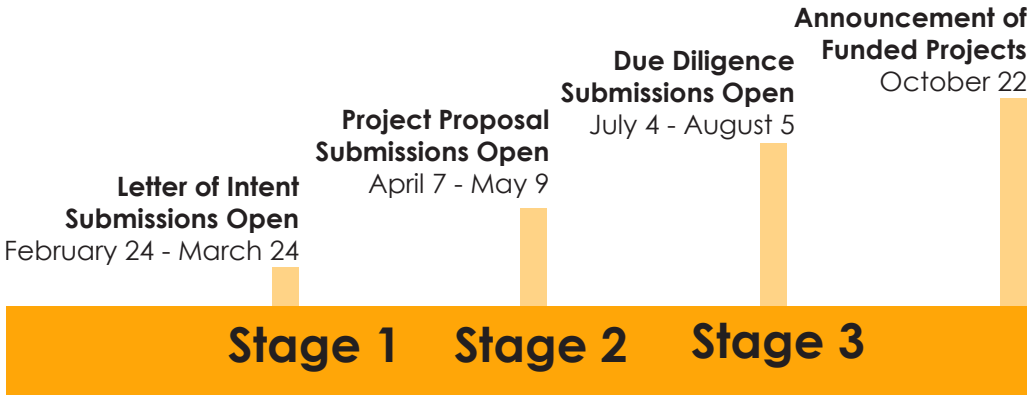
Category 2, New 2025 Projects: An open call for cybersecurity and privacy-related projects; and

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.

Categories 1 and 2 follow a three-stage application and assessment process where submissions are reviewed for eligibility, merit and feasibility by both internal staff and external subject matter experts. Projects that have successfully passed through all three stages will be announced in October during Cybersecurity Awareness Month.

Category 3 projects have an abbreviated application and review process with successful projects announced in January 2026.

2025 Call for Proposals Timeline



Category 1 & 2

Category 3

2025
Call for Proposals Information Sessions

To support applicants throughout the various stages and categories of the Call for Proposals, we hosted a series of Information Sessions held on Zoom in both English and French.

Sessions were well attended with over 250 participants having joined, representing organizations from across Canada. The sessions covered topics including general information, stream and category-specific details, and a breakdown of the requirements during different stages of the Call. The sessions also provided a platform for applicants to directly raise questions with an opportunity to learn how to optimize their applications.

Outreach & Engagement

Throughout 2024-2025 fiscal year, the NCC engaged in many events that cultivated collaboration and capacity-building within the Canadian cybersecurity and privacy ecosystem, a few of which included:

CARA Conference, May 14, 2024, Calgary, AB - Dr. Ken Barker, NCC Scientific Director conducted a presentation entitled, "Upholding Research – Not Holding it Up" at the Canadian Association of Research Administrators Conference.

ORION Think Conference, October 16 and 17, 2024, Blue Mountains, ON – Dr. Charmaine Dean, NCC Chair of the Board and Dr. Steven Liss, NCC Board Director, sat on a panel entitled, "The Intersection of Education and Cybersecurity".

Canada 157: The Canadian National Conference on Innovation, November 7 - 8, 2024, Université du Québec en Outaouais, Gatineau-Ottawa, QC - Dr. Ken Barker, NCC Scientific Director conducted a presentation entitled, "On Advancing the Canadian Cybersecurity Ecosystem".

NCC Conferences & Events

Scientific & Ecosystem Advisory Committee

The NCC has now established an advisory committee called the Scientific & Ecosystem Advisory Committee (SEAC) to advance its goals by providing strategic insights about current trends, challenges, and potential directions that will allow the NCC to impact most effectively cybersecurity in Canada. SEAC is composed of key cybersecurity and privacy experts and leaders drawn from academia, the private sector, not-for-profits, and governments. SEAC will provide advice about where the most pressing needs are across the Canadian cybersecurity ecosystem and how those needs are situated within the larger international setting. SEAC will provide the NCC with insight regarding the changing scope of cybersecurity research, activity, and delivery across its various activities.

SEAC provides advice to the NCC's Scientific Director in identifying strategic scientific and ecosystem imperatives for further research and direction by providing input on a strategic vision and identifying priorities to best serve Canada's cybersecurity needs. It will review, identify, and recommend ways and means for the NCC to deal with scientific strategic and ecosystem objectives for cybersecurity initiatives in Canada. It will provide advice about how to identify potential funding sources for commercialization, training, research & development, and industry collaboration. SEAC will help us promote strong linkages between the NCC and various sectors such as government, public institutions, the security intelligence and law enforcement community, and the private sector. It will help identify potential focused calls-for-proposal and identify sector-based strategic opportunities for the NCC as opportunities present themselves. Members may also play a role in evaluating grant applications based on individual expertise and interests.

SEAC will be a key strategic asset for the NCC and members will be engaged in wider ecosystem to both collect emerging challenges and provide direction for how to address them. We highly value those who have agreed to serve on the initial SEAC committee and will expand upon it over the upcoming year to maximize its value to the NCC and wider ecosystem.

Equity, Diversity, Inclusion & Accessibility

The NCC believes that it can best achieve its mission and vision when it draws on the skills, talents, and perspectives of a diverse group of people with a variety of viewpoints, experiences, and backgrounds.

Since its inception, the NCC has prioritized implementing principles of Equity, Diversity, Inclusion, and Accessibility into the policies and culture of the organization. Throughout 2024-2025, we continue to uphold goals achieved by the Government of Canada's 50 – 30 Challenge within our staff and board. We also continue to integrate EDI considerations into the Call for Proposals submission framework and always strive to develop communications in a way that adheres to accessibility best practices.

Intellectual Property & Partnerships Report

As part of the NCC's staff, the Intellectual Property and Partnership (IP&P) team have been focused on catalysing collaboration across Canada's cybersecurity innovation ecosystem. The team links the NCC to Canadian cybersecurity activities and key regional, sectoral, and institutional stakeholders critical to building Canada's cyber resilience.

The IP&P team's central goal is strengthening the NCC's ecosystem intelligence by translating engagements into initiatives that align public and private leadership and addressing emerging cybersecurity challenges. The team has connected with private sources of capital to acknowledge their catalytic role in the commercialization of cyber technologies. Engagement with potential investors and industry accelerators has brought to the NCC's attention the acute lack of cybersecurity 'accelerator' capabilities in Canada, and inspired workshop topics at the upcoming NCC's 2025 Conference in Banff.

The IP&P team further sought alignment with several industries on data governance, talent development, and the challenges facing CISO and CIOs with intense pressure to 'innovate' in the face of emergent quantum technologies, and broader national innovation policies. In attending the Canadian Science Policy Conference in November in Ottawa, the NCC sees the need for better alignment with industrial policy relating to cybersecurity. It also highlighted possible opportunities in the innovation policy sector relating to the economic importance of cybersecurity for securing economic infrastructure.

In 2025, the IP&P team is working closely with the NCC's Scientific and Ecosystem Advisory Committee (SEAC) to enable the expertise and networks to spur new initiatives with the Canadian cybersecurity and privacy ecosystem.

Membership

The NCC is continually grateful for our members. NCC base membership is open to Canadian organizations from academia, private industry, and the not-for profit sector; and in the past year we saw significant growth in the member complement. Beginning with the founding members from the founding universities that have been NCC members since inception, membership expanded to 54 members for the 2024-25 membership year.

The significant growth of the membership complement helps to uplift an essential goal of the NCC. This network of cybersecurity and privacy leaders and experts from NCC member organizations across Canada supports the NCC in its core directive to strengthen cybersecurity in Canada.

We are deeply appreciative of the important organizations that supported the NCC in the 2024-25 membership year:

2313090 Alberta Ltd.
Actua
Carleton University
Ciptor IT-SAFE Canada Inc.
Concordia University (Founding Member)
Concordia University of Edmonton
CyberSci Cyber Security Challenge Canada
Dalhousie University
DarkCheck
Deloitte
Durham College Of Applied Arts & Technology
École Polytechnique de Montréal
ENFOCOM International Corporation
EnStream LP
Ericsson Canada Inc.
ezSec Inc
Field Effect Software
Fields Institute for Research in the Mathematical Sciences
Humber College Institute of Technology and Advanced Learning
INETCO Systems Limited
Information And Communications Technology Council of Canada Inc.
Institut national de la recherche scientifique
Laboratoire de confiance numérique du Canada - Digital Trust Laboratory of Canada
Lethbridge College
Magnificus Software Inc.
Manitoba Research Network
McGill University
Memorial University of Newfoundland
Palitronica
Portage Cybertech Inc.
Private AI Inc.
Protexxa Inc.
Qohash Inc.
Quantized Technologies Inc.
Quantum Algorithms Institute
Queen's University
RESTIV Technology Inc.
Le Réseau d'Informations Scientifiques du Québec
Saskatchewan Polytechnic
Simon Fraser University
Southern Alberta Institute of Technology
TerraHub Technologies Inc.
Toronto Metropolitan University (Founding Member)
Université Laval
Université de Sherbrooke
University of British Columbia
University of Calgary
University of Guelph
University of New Brunswick
University of Ontario Institute of Technology
University Ottawa
University Quebec Outaouais
University of Saskatchewan
University of Waterloo
University of Western Ontario
Valencia IIP Advisors Limited
VanWyn Inc.
York University


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

NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

www.ncc-cnc.ca

[Follow us on LinkedIn]

[Sign-up for our mailing list]

Funded by the Government of Canada
Financé par le gouvernement du Canada

Canada