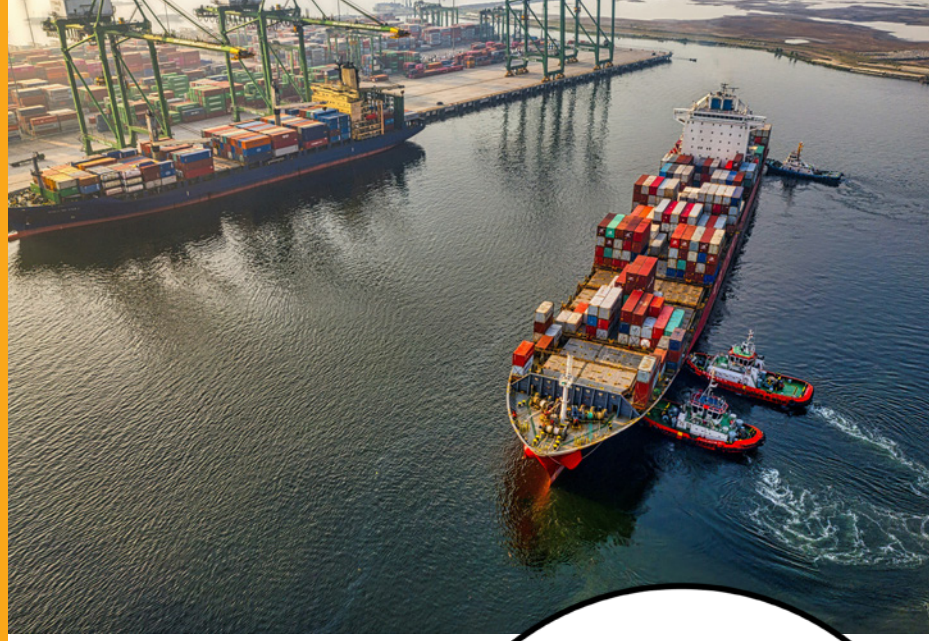
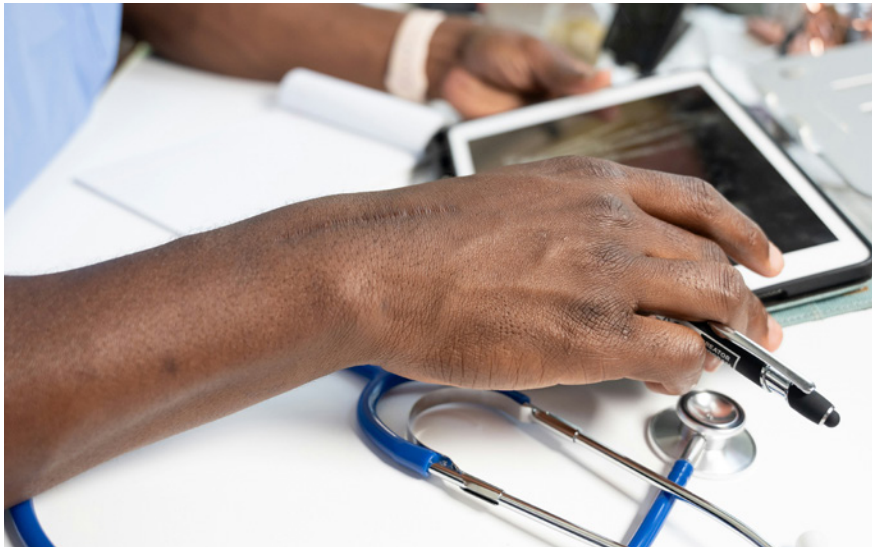


NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

Rapport annuel 2024 - 2025



Message de la présidente du conseil d'administration

Charmaine Dean, Ph. D.

La cybersécurité continue d'être un sujet primordial au quotidien au Canada. Le Consortium national pour la cybersécurité (CNC) a été créé dans le but de renforcer l'écosystème de la cybersécurité du Canada et de soutenir des initiatives de pointe visant à protéger les Canadiennes et les Canadiens. Chaque jour, le CNC apporte son soutien à notre communauté et aux projets que nous finançons dans le cadre de notre engagement envers l'amélioration de la cybersécurité au Canada.

Le CNC et la demande pour du soutien financier ont connu une croissance considérable au cours de notre deuxième année d'activité. En 2024, nous avons reçu plus de 90 demandes de financement et avons apporté notre soutien à 37 projets canadiens d'envergure dans le domaine de la cybersécurité en offrant plus de 22 millions $ en financement. La nécessité d'avoir des secteurs de la recherche, du développement, de la formation et de la commercialisation de la cybersécurité adéquatement financés et à la fine pointe de la technologie est bien démontrée.

Le CNC et son équipe ont travaillé avec assiduité pour devenir reconnus comme l'un des acteurs les plus actifs et les plus essentiels de l'écosystème de la cybersécurité au Canada. Sous la direction de notre directeur scientifique, Ken Barker, notre équipe dévouée travaille d'arrache-pied pour offrir des programmes efficaces et efficients et pour bâtir un bassin pancanadien et interdépendant de membres experts en cybersécurité. En collaboration avec nos partenaires du Réseau d'innovation pour la cybersécurité d'Innovation, Sciences et Développement économique Canada, le CNC offre d'agir à titre de point de contact indispensable pour l'élaboration de programmes de cybersécurité dans les champs de la recherche, de la formation et de la commercialisation. L'année 2024-2025 fut marquée par le développement de notre communauté et l'élargissement de notre portée auprès d'un groupe d'acteurs canadiens de la cybersécurité en constante expansion dans le monde académique et le secteur privé.

Je tiens à remercier mes collègues membres du conseil d'administration du CNC et toute l'équipe du CNC pour leurs services rendus à cet environnement marqué par l'innovation. Au cours de la dernière année, votre dévouement et votre créativité ont été essentiels au succès du CNC et c'est pour moi un honneur de travailler avec vous.

Sincèrement,

Charmaine Dean

Conseil d'administration

Amir Belkhelladi
associé et leader national, Services liés aux cyberrisques, Deloitte

Effrosyni Diamantoudi, Ph. D.
doyenne des études supérieures, Université Concordia

William Ghali, Ph. D.
vice-président, recherche, Université de Calgary

Elaine Hum
directrice, partenariats de cybersécurité, Scotiabank

Emily Laidlaw, Ph. D.
professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité, Faculté de droit, Université de Calgary

Steven N. Liss, Ph. D.
vice-président, recherche et innovation, Université métropolitaine de Toronto

David MaGee, Ph. D.
vice-président, recherche, Université du Nouveau-Brunswick

Greg Murray
SVP, cybersécurité, vie privée et réseaux, Les Compagnies Loblaw limitée

Message du directeur scientifique

du Consortium national pour la cybersécurité

Ken Barker Ph. D.

Le CNC a eu une année très excitante et très productive! Nous sommes partis d'une vision et en avons fait une réalité qui transforme l'écosystème de la cybersécurité au Canada.

Cette année fut notre première année complète d'activités. Nous avons tenu la première ronde de financement du Réseau d'innovation pour la cybersécurité (RIC) et réalisé notre appel à proposition 2024. Celle-ci avait pour but de cibler des initiatives méritoires en matière de cybersécurité et de protection de la vie privée en soutien aux intérêts du Canada et à la protection des Canadiennes et des Canadiens.

Le CNC dispose désormais de tout le personnel nécessaire à la réalisation de ses activités. Le groupe fournit à nos parties prenantes des services de la plus haute qualité pour s'assurer que celles-ci permettent à nos responsables de projet d'atteindre leurs objectifs, notamment en ce qui concerne les programmes de formation, les initiatives de recherche et de développement et la commercialisation d'idées novatrices. Notre équipe a adopté une devise : « Soutenir la recherche, et non la retenir! »

Nous tenons à remercier les nombreux participants du secteur privé et du secteur public, notamment nos parties prenantes issues du milieu de l'enseignement supérieur. De plus, le CNC est très reconnaissant de l'appui important du gouvernement fédéral, qui nous a permis d'atteindre nos objectifs et nous a aidés maintes et maintes fois à trouver des solutions pour que les choses se fassent. De même, je tiens à remercier l'ensemble de la communauté des experts en informatique de tous les secteurs pour leurs contributions au CNC, notamment pour leurs conseils, leurs examens des projets, leur appui aux demandes de financement et leur soutien moral alors que nous mettions sur pied le CNC.

Je souhaite également remercier notre conseil d'administration pour son engagement inébranlable à l'égard du CNC, de ses objectifs et de sa vision, ainsi que notre personnel qui continue de travailler dur pour établir une approche véritablement visionnaire afin de répondre à un besoin fondamental au Canada. Votre vision, votre engagement et votre expertise permettront au CNC de prospérer et de diversifier sa proposition de valeur à l'intention de ses membres alors que nous entamons notre troisième année complète d'activité.

Les nouvelles possibilités en matière d'IA et d'informatique quantique, que nous intégrons à notre réflexion sur la cybersécurité et la protection de la vie privée au Canada, se classent selon deux axes : premièrement, ces technologies peuvent servir d'outils pour une sécurité améliorée et une meilleure protection de la vie privée à travers les techniques en développement; et deuxièmement, la menace que constitue l'émergence et l'arrivée à maturité de ces technologies présentent de nouveaux défis à relever au fur et à mesure de leur déploiement. Le CNC est d'avis qu'il doit jouer un rôle de chef de file pour ces deux dimensions en tirant parti de son expertise approfondie en matière de cybersécurité et de protection de la vie privée pour s'assurer que l'IA et l'informatique quantique soient appliquées le plus efficacement possible aux défis et aux possibilités du Canada en matière d'activités numériques. Des investissements importants sont faits pour développer l'IA et l'informatique quantique au Canada. Par conséquent, il est nécessaire de faire des investissements correspondants pour comprendre les menaces et les possibilités que ces technologies présentent grâce à l'expertise de l'ensemble des membres du CNC. Ultimement, les investissements en cybersécurité devront provenir de sources publiques et privées.

Sincèrement,

Ken Barker

Appel à propositions

2024

Lors de son deuxième appel à propositions, le CNC a octroyé 21,4 millions $ pour financer 36 projets distincts, tirant des contributions financières et techniques d'organisations établies partout au Canada. Ce montant porte le total des sommes octroyées en financement pour ce projet en cybersécurité canadienne à plus de 54 millions $.

Le programme de financement annuel du CNC a pour but de stimuler un écosystème national solide de cybersécurité et de positionner le Canada comme chef de file mondial en matière de cybersécurité. Depuis 2023, le CNC a financé trois catégories de projets du domaine de la cybersécurité : commercialisation, recherche et développement et formation. Ces projets représentent des secteurs d'activité variés, allant de la construction d'un réseau 5G sécurisé et cyberrésilient au moyen de l'IA à l'offre d'un programme de maîtrise en cybersécurité.

Projets 2024 retenus

Recherche et développement – De pointe

Protection de la vie privée des enfants canadiens : un cadre sûr et sécurisé pour les grands modèles de langage

Bénéficiaire : Université Carleton, Ottawa (Ont.)

Fonds mobilisés par le CNC : 88 800 $

Plateforme à vérification systématique à l'échelle de l'entreprise pour la création de services de comptage intelligents renforçant le respect de la vie privée

Bénéficiaire : Université du Nouveau-Brunswick, Fredericton (N.-B.)

Fonds mobilisés par le CNC : 90 390 $

Sécuriser le métavers au moyen de méthodes de contrôle d'accès et d'authentification multimodales

Bénéficiaire : Institut national de la recherche scientifique, Québec (Qc)

Collaborateurs : In Virtuo, Beam Me Up, Kaptics, MYND Therapeutics, Université de Waterloo, ColAB Numérique, Digital Trust

Fonds mobilisés par le CNC : 500 000 $

Améliorer la cybersécurité de l'infrastructure de recharge des véhicules électriques grâce à une IA autonome et durable

Bénéficiaire : Institut de technologie de l'Université de l'Ontario, Oshawa (Ont.)

Collaborateurs : Université Western

Fonds mobilisés par le CNC : 175 294,10 $

Comptabilité en mode autruche : régler les détails, la tête dans le sable

Bénéficiaire : Université de Calgary, Calgary (Alb.)

Fonds mobilisés par le CNC : 500 000 $

Découverte et réparation entièrement automatisées des vulnérabilités de bout en bout grâce aux GML

Bénéficiaire : Université Simon Fraser, Burnaby (C.-B.)

Fonds mobilisés par le CNC : 500 000 $

Renforcer la cyberrésilience des miniréseaux dans les futures infrastructures énergétiques essentielles

Bénéficiaire : Université Concordia, Montréal (Qc)

Collaborateurs : RMDS Innovation Inc., Université du Nouveau-Brunswick

Fonds mobilisés par le CNC : 352 940 $

Système de défense décisionnelle adaptatif : une approche proactive de la détection et de l'atténuation des attaques par double déni de décision dans les infrastructures essentielles

Bénéficiaire : Université de Calgary, Calgary (Alb.)

Collaborateurs : Université de Guelph, Université Laval, CyberPatterns Inc., Waterfall Security Solutions

Fonds mobilisés par le CNC : 496 800 $

La sécurité des SCI à l'ère de l'industrie 4.0

Bénéficiaire : University of British Columbia, Vancouver, BC

Fonds mobilisés par le CNC : 500 000 $

Protéger la démocratie des cybermenaces

Bénéficiaire : Université de Calgary, Calgary (Alb.)

Fonds mobilisés par le CNC : 500 000 $

Préserver la confidentialité des relations dans les grands réseaux

Bénéficiaire : Université de la Colombie-Britannique, Vancouver (C.-B.)

Fonds mobilisés par le CNC : 500 000 $

Nouvelles méthodes de quantification et d'amélioration du respect de la vie privée dans l'apprentissage machine

Bénéficiaire : Université de la Colombie-Britannique, Vancouver (C.-B.)

Fonds mobilisés par le CNC : 495 000 $

Renforcer la cybersécurité : méthodes de détection précoce et d'atténuation des rançongiciels

Bénéficiaire : Université du Nouveau-Brunswick, Fredericton (N.-B.)

Collaborateurs : Université d'Ottawa, Bell Canada, EzSec

Fonds mobilisés par le CNC : 79 500 $

Lutte contre les opérations de cyberinfluence sur les médias sociaux

Bénéficiaire : Université Laval, Québec (Qc)

Collaborateurs : Université McGill, Université du Manitoba

Fonds mobilisés par le CNC : 485 875 $

Pare-feu IA adaptatif spécialisé dans la protection des modèles, infrastructures essentielles, systèmes et agents d'IA

Bénéficiaire : Université Western, London (Ont.)

Collaborateurs : Syngen AI Lab, Université de Waterloo

Fonds mobilisés par le CNC : 500 000 $

Formation à la sensibilisation à la sécurité par l'apprentissage social en ligne – de l'hameçonnage à l'hameçonnage vocal en passant par l'hameçonnage par SMS

Bénéficiaire : Université d'Ottawa, Ottawa (Ont.)

Collaborateurs : Gendarmerie royale du Canada

Fonds mobilisés par le CNC : 373 500 $

Assurer la sécurité vitale : coordination de groupes de drones autonomes avec prise de décision pesant les facteurs de sécurité

Bénéficiaire : Université d'Ottawa, Ottawa (Ont.)

Collaborateurs : Quanser, Université Concordia

Fonds mobilisés par le CNC : 499 100 $

Évaluation de la cybersécurité de modèles prédéploiement de systèmes industriels

Bénéficiaire : Université de Sherbrooke, Sherbrooke (Qc)

Collaborateurs : Centris Technologies, Neverhack, Productique Québec

Fonds mobilisés par le CNC : 480 000 $

Traitement sécurisé des données génomiques : libérer le potentiel de la médecine personnalisée

Bénéficiaire : Université de Waterloo, Waterloo (Ont.)

Collaborateurs : Chercheur autonome en génomique indiqué

Fonds mobilisés par le CNC : 129 900 $

Stratégies de défense adaptatives pour les systèmes avancés d'aide à la conduite : une approche théorique des jeux

Bénéficiaire : Université de Waterloo, Waterloo (Ont.)

Fonds mobilisés par le CNC : 164 622,50 $

Adversaires transformateurs : exploitation des transformateurs génératifs préentraînés pour la création de moteurs de maliciels métamorphiques de nouvelle génération

Bénéficiaire : Institut de technologie de l'Université de l'Ontario, Oshawa (Ont.)

Fonds mobilisés par le CNC : 382 352,94 $

Solution de cybersécurité de bout en bout pour le réseau électrique

Bénéficiaire : Université York, Toronto (Ont.)

Collaborateurs : Cistel Technology, Siemens Inc., IESO, Université Dalhousie, Université Carleton

Fonds mobilisés par le CNC : 300 000 $

Recherche et développement – Standard

Permettre l'externalisation sécurisée de données sensibles

Bénéficiaire : Université de Waterloo, Waterloo (Ont.)

Collaborateurs : Amazon AWS, Banque Royale du Canada, Airbus

Fonds mobilisés par le CNC : 295 000 $

Authentification pour les communications quantiques sécurisées

Bénéficiaire : Quantized Technologies Inc, Calgary (Alb.)

Collaborateurs : Université de Calgary

Fonds mobilisés par le CNC : 940 000 $

IntruderInsight : améliorer la cyberattribution grâce aux renseignements dérivés de l'IA

Bénéficiaire : ENFOCOM International Corporation, Calgary (Alb.)

Collaborateurs : Université de Calgary – département d'informatique , Field Effect Software Inc., Raytheon Canada, Cybera, Gendarmerie royale du Canada, Services de police de Calgary, Services de police d'Edmonton, IBM Canada, Université du Québec en Outaouais, Intlabs, Check Point Software Technologies, InceptionU Educational Foundation Ltd., Raytheon Canada, Université du Nouveau-Brunswick, Université métropolitaine de Toronto – Rogers Cybersecure Catalys

Fonds mobilisés par le CNC : 2 000 000 $

Vers un système sécurisé de gestion des crédits d'énergie verte centré sur l'utilisateur

Bénéficiaire : Université de Calgary, Calgary (Alb.)

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

Fonds mobilisés par le CNC : 561 000 $

Révolutionner la cybersécurité personnelle grâce aux renseignements dérivés de l'IA

Bénéficiaire : Protexxa Inc, Aurora (Ont.)

Collaborateurs : Université métropolitaine de Toronto, Core Centre Inc, Mila Montreal

Fonds mobilisés par le CNC : 1 701 280 $

SCMS : sécurisation des systèmes maritimes critiques

Bénéficiaire : Université Memorial de Terre-Neuve, St. John's (T.-N.-L.)

Collaborateurs : Université Dalhousie, Recherche et développement pour la défense Canada, Institut marin, Transports Canada

Fonds mobilisés par le CNC : 759 073,18 $

Commercialisation

CyberGuardian : combler le fossé de formation dans le contexte de la lutte contre la cybersécurité

Bénéficiaire : ENFOCOM International Corporation, Calgary (Alb.)

Collaborateurs : Raytheon Canada, Université de Calgary, Gendarmerie royale du Canada, Service de police de Calgary, Service de police d'Edmonton, Check Point Software Technologies, InceptionU Educational Foundation Ltd., Université d'Ottawa, Field Effect Software Inc.,IBM Canada

Fonds mobilisés par le CNC : 1 000 000 $

Commercialisation C1R3

Bénéficiaire : Portage CyberTech Inc, Gatineau (Qc)

Collaborateurs : Converger, Centre de recherche et développement expérimental en informatique libre – CREDIL, Université du Québec en Outaouais, Université McGill, Zu, Flex Groups,

Fonds mobilisés par le CNC : 1 000 000 $

Formation

IncidentSync : faire le lien entre les technologies de l'information et les forces de l'ordre

Bénéficiaire : ENFOCOM International Corporation, Calgary (Alb.)

Collaborateurs : Field Effect Software Inc., Université métropolitaine de Toronto - Rogers Cybersecure Catalyst, Gendarmerie royale du Canada, Services de police de Calgary, Services de police d'Edmonton, Université de Calgary - Éducation permanente, InceptionU Educational Foundation Ltd, Intlabs, Université du Québec en Outaouais, Savvy Knowledge Corporation, Raytheon Canada, IBM Canada, Check Point, Software Technologies

Fonds mobilisés par le CNC : $1,000,000

Accélérer les efforts déployés pour sécuriser le Canada à l'ère de l'informatique quantique

Bénéficiaire : Quantum Algorithms Institute, Surrey (C.-B.)

Collaborateurs : Field Effect, Conseil des technologies de l'information et des communications, siberX, Association canadienne de l'informatique, Beauceron Security, Quantum Algorithms Institute, Collège Durham

Fonds mobilisés par le CNC : 1 000 000 $

Formation immersive à la cybersécurité centrée sur l'être humain : conséquences socio-techniques et juridiques d'une attaque

Bénéficiaire : Université d'Ottawa, Ottawa (Ont.)

Collaborateurs : Université de Montréal, Université de Calgary, ENFOCOM, Field Effect, IBM, Desjardins, BNC (à confirmer)

Fonds mobilisés par le CNC : 961 400 $

La robotique cybersécurisée et les talents de demain

Bénéficiaire : Université de Waterloo, Waterloo (Ont.)

Collaborateurs : Cobionics, Labforge, Laboratoires Nucléaires Canadiens, BTQ, Palitronica, Quanser, Alectra, Milton Hydro, Real Life Robotics

Fonds mobilisés par le CNC : 1 000 000 $

Formation à la cybersécurité maritime

Bénéficiaire : Université Memorial de Terre-Neuve, St. John's (T.-N.-L.)

Collaborateurs : Thales

Fonds mobilisés par le CNC : 1 000 000 $

Formation pour une cybersécurité proactive et interdisciplinaire en entreprise

Bénéficiaire : Université de Sherbrooke, Sherbrooke (Qc)

Collaborateurs : Cybereco, Intact corporation financière

Fonds mobilisés par le CNC : $ 580 679

Appel à propositions 2025

Le CNC a octroyé plus de 20 millions de dollars pour des projets de cybersécurité au Canada dans le cadre du troisième appel à propositions.

Pour l'appel à propositions de 2025, le CNC a constitué trois nouvelles catégories afin d'accueillir différents types de projets issus de l'écosystème de cybersécurité et de protection de la vie privée au Canada. Voici ces nouvelles catégories de financement :

Catégorie 1, projets accélérés : destiné à faire avancer rapidement des projets très ciblés et associés à un budget important;

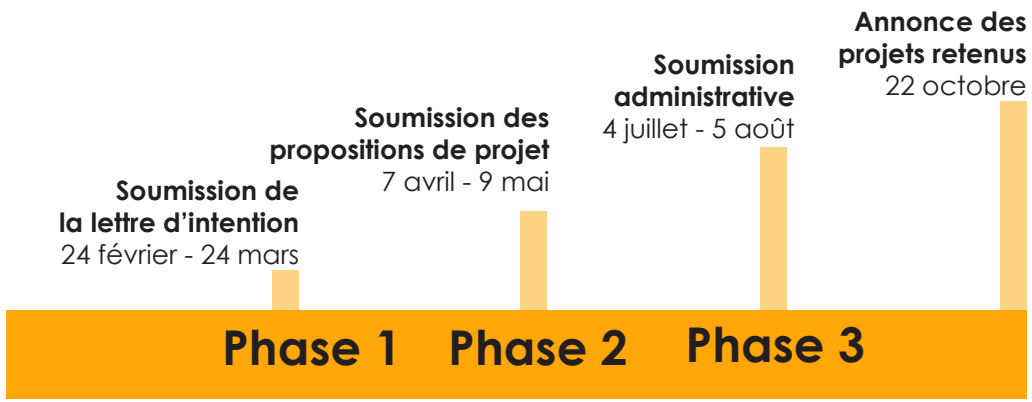
Catégorie 2, nouveaux projets pour 2025 : un appel à propositions pour des initiatives axées sur la cybersécurité et la protection de la vie privée;

Catégorie 3, financement additionnel pour les projets de 2023/2024 : destiné à renforcer les résultats des projets déjà approuvés par le CNC en leur permettant d'intégrer de nouvelles idées ou de remédier aux lacunes identifiées lors des travaux menés jusqu'à présent.

Les catégories 1 et 2 suivent un processus de candidature et d'évaluation en trois étapes dans le cadre duquel les projets soumis sont examinés par le personnel interne et des experts externes pour en déterminer l'admissibilité, le bien-fondé et la faisabilité. Les projets qui passent les trois étapes avec succès seront annoncés en octobre au cours du Mois de la sensibilisation à la cybersécurité.

Quant à eux, les projets relevant de la catégorie 3 bénéficient d'un processus de soumission et d'examen accéléré et les projets retenus seront annoncés en janvier 2026.

2025 Calendrier de l'appel à propositions



Catégorie 1 & 2

Catégorie 3

Séances d'information sur les appels à propositions

2025

Nous avons organisé une série de séances d'information sur Zoom en français et en anglais pour soutenir les candidates et les candidates tout au long des différentes étapes et pour les différentes catégories de l'appel à propositions.

Plus de 250 personnes, représentant des organismes de partout au Canada, ont participé aux séances. De nombreux sujets furent couverts dans le cadre de ces séances, notamment des renseignements généraux, les détails spécifiques aux volets et une présentation des exigences associées aux différentes étapes de l'appel à propositions. Les séances ont également permis aux demandeurs de poser directement des questions et d'apprendre à optimiser leurs dossiers de candidature.

Diffusion et mobilisation

Tout au long de l'exercice 2024-2025, le CNC a pris part à de nombreux événements visant à renforcer la collaboration et les compétences au sein de l'écosystème canadien de la cybersécurité et de la protection de la vie privée.

Conférence de l'ACAAR,14 mai 2024, Calgary, Alberta : M. Ken Barker, directeur scientifique du CNC, a donné une présentation intitulée « Upholding Research – Not Holding it Up » (Soutenir la recherche, et non la retenir)

Conférence ORION Think, 16 et 17 octobre 2024, Blue Mountains, Ontario : Mme Charmaine Dean, présidente du conseil d'administration du CNC, et M. Steven Liss, administrateur au sein du conseil d'administration du CNC, ont participé à un panel intitulé « The Intersection of Education and Cybersecurity » (L'intersection entre l'éducation et la cybersécurité)

Canada 157 : La conférence nationale sur l'innovation au Canada, 7-8 novembre 2024, Université du Québec en Outaouais, Gatineau-Ottawa, Québec : M. Ken Barker, directeur scientifique du CNC, a donné une présentation intitulée, « On Advancing the Canadian Cybersecurity Ecosystem » (De l'amélioration de l'environnement de la cybersécurité au Canada)

Conférences et événements

Comité consultatif scientifique et de l'écosystème

Le CNC a mis sur pied un comité appelé le Comité consultatif scientifique et de l'écosystème (CCSE) afin de promouvoir ses objectifs en fournissant des analyses stratégiques concernant les tendances actuelles, les défis et les orientations potentielles qui pourraient permettre au CNC d'avoir l'incidence la plus efficace possible dans le domaine de la cybersécurité au Canada. Le CCSE est composé d'experts en cybersécurité et en protection de la vie privée et de leaders issus du monde académique, du secteur privé, d'organismes à but non lucratif et des gouvernements. Le CCSE a le mandat de fournir des conseils pour déterminer les domaines où se trouvent les besoins les plus pressants dans l'écosystème canadien de cybersécurité et sur la position de ces besoins par rapport au contexte international. Le CCSE doit fournir au CNC des observations sur l'évolution de la portée de la recherche, des activités et des résultats en matière de cybersécurité dans le cadre de ses diverses activités.

Concrètement, le CCSE doit conseiller le directeur scientifique du CNC pour l'aider à cibler des impératifs stratégiques scientifiques et écosystémiques favorisant l'avancement de la recherche ainsi que les orientations à adopter, en apportant sa perspective à la vision stratégique et en relevant les priorités qui répondent le mieux aux besoins du Canada en matière de cybersécurité. Son mandat consiste notamment à examiner, cibler et recommander des moyens qui permettront au CNC d'atteindre les objectifs scientifiques stratégiques et écosystémiques liés aux initiatives de cybersécurité au Canada. Il fournira aussi des conseils sur la manière de trouver des sources de financement pour la commercialisation, la formation, la recherche et le développement ainsi qu'en matière de collaboration avec les acteurs de l'industrie.

Par ailleurs, le CCSE nous aidera à établir des liens solides entre le CNC et divers secteurs tels que les gouvernements, les institutions publiques, le secteur du renseignement de sécurité et de l'application de la loi et le secteur privé. Il aidera à cerner des propositions ciblées et à identifier les possibilités stratégiques sectorielles pour le CNC à mesure que les occasions se présentent. Les membres pourront également jouer un rôle dans l'évaluation des demandes de financement en fonction de leurs expertises et champs d'intérêt.

Ainsi, le CCSE sera un actif stratégique clé pour le CNC. Ses membres interagiront avec l'écosystème plus vaste afin de cibler les nouveaux défis et de fournir des solutions pour les relever. Nous accordons une grande valeur aux personnes qui ont accepté d'occuper un poste au sein du premier comité. Nous prévoyons élargir la portée du comité au cours de l'année à venir afin d'en maximiser la valeur pour le CNC et l'écosystème de la cybersécurité en général.

Nouvelles sur l'équité, la diversité, l'inclusion et l'accessibilité

Le CNC croit qu'il est le mieux à même de réaliser sa mission et sa vision lorsqu'il s'appuie sur les compétences, les talents et les perspectives d'un groupe diversifié de personnes ayant des points de vue, des expériences et des parcours variés.

Depuis sa fondation, le CNC a fait une priorité de l'intégration des principes d'équité, de diversité, d'inclusion et d'accessibilité à ses politiques et sa culture organisationnelle. Tout au long de l'année 2024-2025, nous avons continué de maintenir les cibles établies par le Défi 50-30 du gouvernement du Canada pour les membres de notre personnel et de notre conseil d'administration. Nous continuons également d'intégrer les principes de DEI dans le processus d'appel à propositions et cherchons toujours à formuler nos communications conformément aux meilleures pratiques en matière d'accessibilité.

Rapport sur la propriété intellectuelle et les partenariats

L'équipe de la propriété intellectuelle et des partenariats du CNC s'est concentrée sur la promotion de la collaboration dans l'ensemble de l'écosystème canadien d'innovation en cybersécurité. L'équipe fait le pont entre le CNC et les activités de cybersécurité au Canada et les principaux acteurs régionaux, sectoriels et institutionnels essentiels pour renforcer la cyberrésilience du Canada.

L'objectif clé de l'équipe de la propriété intellectuelle et des partenariats du CNC est de renforcer la connaissance de l'écosystème en transformant les engagements en initiatives visant à arrimer les leaderships public et privé et à relever les défis émergents en matière de cybersécurité. L'équipe a ainsi établi des relations avec des sources privées de capitaux pour reconnaître leur rôle catalyseur dans la commercialisation des cybertechnologies. Les discussions avec des investisseurs potentiels et des accélérateurs de l'industrie ont attiré l'attention du CNC sur les carences aiguës dans l'offre d'accélérateurs d'entreprises du domaine de la cybersécurité au Canada et ont inspiré des thèmes d'atelier pour la prochaine conférence du CNC qui aura lieu à Banff en 2025.

L'équipe de la propriété intellectuelle et des partenariats a également cherché à arrimer sa position avec celles de plusieurs industries sur la gouvernance des données, le développement des talents et les défis auxquels sont confrontés les responsables de la sécurité de l'information et les responsables des technologies de l'information, notamment la pression intense à « innover » face aux technologies quantiques émergentes ainsi que les politiques nationales d'innovation plus générales. Lors de sa participation à la Conférence sur les politiques scientifiques canadiennes, qui a eu lieu en novembre à Ottawa, le CNC a constaté la nécessité d'une meilleure harmonisation avec la politique industrielle en matière de cybersécurité. Cet événement a également mis en lumière les possibilités qui s'offrent dans le secteur des politiques d'innovation et de l'importance économique de la cybersécurité pour la sécurité des infrastructures économiques.

En 2025, l'équipe de la propriété intellectuelle et des partenariats a travaillé en étroite collaboration avec le Comité consultatif scientifique et de l'écosystème (CCSE) du CNC pour permettre aux experts et aux réseaux de mettre sur pied de nouvelles initiatives au sein de l'écosystème de cybersécurité et de protection de la vie privée au Canada.

Rapport sur les membres

Le CNC tient à exprimer sa reconnaissance envers ses membres. L'adhésion de base au CNC est ouverte aux organisations du monde académique, du secteur privé et du secteur des organismes à but non lucratif et nous avons vu une importante croissance du nombre de membres. En tenant compte des membres fondateurs des universités fondatrices qui sont membres du CNC depuis sa création, le nombre de membres est passé à 54 pour l'année 2024-2025.

La croissance importante du nombre de membres contribue à l'atteinte d'un objectif essentiel pour le CNC. Ce réseau de leaders du domaine de la cybersécurité et de la protection de la vie privée et d'experts issus des organismes membres du CNC de partout au Canada appuient le CNC dans sa mission fondamentale qui consiste à renforcer la cybersécurité au Canada.

Nous sommes profondément reconnaissants des organisations importantes qui ont soutenu le travail du CNC au cours de l'année 2024-2025 :

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


Les bonnes personnes,
les bons échanges,
au bon moment

NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

www.ncc-cnc.ca

Suivez-nous sur LinkedIn

Inscrivez-vous à notre liste d'envoi

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

Canada

Consortium national pour la cybersécurité
États financiers
Pour l'exercice terminé le 31 mars 2025

Table des matières

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

Rapport de l'auditeur indépendant

Aux membres du
Consortium national pour la cybersécurité

Opinion

Nous avons effectué l'audit des états financiers du Consortium national pour la cybersécurité (le « consortium »), qui comprennent l'état de la situation financière au 31 mars 2025, et les états des résultats, de l'évolution de l'actif net (insuffisance) et des flux de trésorerie pour l'exercice terminé à cette date, ainsi que les notes, y compris le résumé des principales méthodes comptables.

À notre avis, les états financiers ci-joints donnent, dans tous leurs aspects significatifs, une image fidèle de la situation financière du consortium au 31 mars 2025, ainsi que de sa performance financière et de ses flux de trésorerie pour l'exercice terminé à cette date, conformément aux Normes comptables canadiennes pour les organismes sans but lucratif.

Fondement de l'opinion

Nous avons effectué notre audit conformément aux normes d'audit généralement reconnues du Canada. Les responsabilités qui nous incombent en vertu de ces normes sont plus amplement décrites dans la section *Responsabilités de l'auditeur à l'égard de l'audit des états financiers* du présent rapport. Nous sommes indépendants du consortium conformément aux règles de déontologie qui s'appliquent à notre audit des états financiers au Canada et nous nous sommes acquittés des autres responsabilités déontologiques qui nous incombent selon ces règles. Nous estimons que les éléments probants que nous avons obtenus sont suffisants et appropriés pour fonder notre opinion d'audit.

Responsabilités de la direction et des responsables de la gouvernance à l'égard des états financiers

La direction est responsable de la préparation et de la présentation fidèle des états financiers conformément aux Normes comptables canadiennes pour les organismes sans but lucratif, ainsi que du contrôle interne qu'elle considère comme nécessaire pour permettre la préparation d'états financiers exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs.

Lors de la préparation des états financiers, c'est à la direction qu'il incombe d'évaluer la capacité du consortium à poursuivre son exploitation, de communiquer, le cas échéant, les questions relatives à la continuité de l'exploitation et d'appliquer le principe comptable de continuité d'exploitation, sauf si la direction a l'intention de liquider le consortium ou de cesser son activité ou si aucune solution réaliste ne s'offre à elle.

Il incombe aux responsables de la gouvernance de surveiller le processus d'information financière du consortium.

Responsabilités de l'auditeur à l'égard de l'audit des états financiers

Nos objectifs sont d'obtenir l'assurance raisonnable que les états financiers pris dans leur ensemble sont exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, et de délivrer un rapport de l'auditeur contenant notre opinion. L'assurance raisonnable correspond à un niveau élevé d'assurance, qui ne garantit toutefois pas qu'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada permettra toujours de détecter toute anomalie significative qui pourrait exister. Les anomalies peuvent résulter de fraudes ou d'erreurs et elles sont considérées comme significatives lorsqu'il est raisonnable de s'attendre à ce que, individuellement ou collectivement, elles puissent influer sur les décisions économiques que les utilisateurs des états financiers prennent en se fondant sur ceux-ci.

Dans le cadre d'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada, nous exerçons notre jugement professionnel et faisons preuve d'esprit critique tout au long de cet audit. En outre :

- Nous identifions et évaluons les risques que les états financiers comportent des anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, concevons et mettons en œuvre des procédures d'audit en réponse à ces risques, et réunissons des éléments probants suffisants et appropriés pour fonder notre opinion. Le risque de non-détection d'une anomalie significative résultant d'une fraude est plus élevé que celui d'une anomalie significative résultant d'une erreur, car la fraude peut impliquer la collusion, la falsification, les omissions volontaires, les fausses déclarations ou le contournement du contrôle interne;
- Nous acquérons une compréhension des éléments du contrôle interne pertinents pour l'audit afin de concevoir des procédures d'audit appropriées aux circonstances, et non dans le but d'exprimer une opinion sur l'efficacité du contrôle interne du consortium;
- nous apprécions le caractère approprié des méthodes comptables retenues et le caractère raisonnable des estimations comptables faites par la direction, de même que des informations y afférentes fournies par cette dernière;
- Nous tirons une conclusion quant au caractère approprié de l'utilisation par la direction du principe comptable de continuité d'exploitation et, selon les éléments probants obtenus, quant à l'existence ou non d'une incertitude significative liée à des événements ou situations susceptibles de jeter un doute important sur la capacité du consortium à poursuivre son exploitation. Si nous concluons à l'existence d'une incertitude significative, nous sommes tenus d'attirer l'attention des lecteurs de notre rapport sur les informations fournies dans les états financiers au sujet de cette incertitude ou, si ces informations ne sont pas adéquates, d'exprimer une opinion modifiée. Nos conclusions s'appuient sur les éléments probants obtenus jusqu'à la date de notre rapport. Des événements ou situations futurs pourraient par ailleurs amener le consortium à cesser son exploitation;
- Nous évaluons la présentation d'ensemble, la structure et le contenu des états financiers, y compris les informations fournies dans les notes, et apprécions si les états financiers représentent les opérations et événements sous-jacents d'une manière propre à donner une image fidèle.

Nous communiquons aux responsables de la gouvernance notamment l'étendue et le calendrier prévus des travaux d'audit et nos constatations importantes, y compris toute déficience importante du contrôle interne que nous aurions relevée au cours de notre audit.

BDO Canada s.r.l./LLP

Comptables professionnels agréés
Ottawa (Ontario)
Le 26 juin 2025

Consortium national pour la cybersécurité
État de la situation financière

31 mars	2025	2024
Actif		
Court terme		
Encaisse	1 516 381 $	1 520 299 $
Comptes à recevoir	191 492	140 823
Autres créances	76 710	46 200
Frais payés d'avance	100 375	26 346
Avances de projets	3 994 276	-
Actif total	5 879 234 $	1 733 668 $
Passif et actif net (insuffisance)		
Court terme		
Créditeurs et frais courus (Note 2)	292 149 $	127 487 $
Subventions à payer - remboursements	1 303 926	-
Subventions à payer - bénéficiaires finaux	952 266	-
Subventions et adhésions reportées (Note 3)	2 999 526	1 513 992
Dû aux membres fondateurs	115 000	112 500
	5 662 867	1 753 979
	5 662 867	1 753 979
Actif net (insuffisance)		
Non affecté	216 367	(20 311)
	216 367	(20 311)
Total du passif et de l'actif net	5 879 234 $	1 733 668 $

Au nom du Conseil d'administration :

Signed by: Charmaine B. Dean
41D0855C03A4474...
Directeur

Signed by: David MacGee
9C036B809005435...
Directeur

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État de l'évolution de l'actif net (insuffisance)

Pour l'exercice terminé le 31 mars 2025	2025	2024
Solde, début de l'exercice	(20 311)$	20 317 $
Excédent (insuffisance) des produits sur les charges	236 678	(40 628)
Solde, fin de l'exercice	216 367 $	(20 311)$

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État des résultats

Pour l'exercice terminé le 31 mars	2025	2024
Produits		
Subventions (Note 2)	5 010 800 $	1 445 318 $
Adhésions (Note 2)	309 862	33 585
Intérêts et autres revenus	24 434	-
	5 345 096	1 478 903
Charges		
Programmes	2 573 147	-
Développement, prestation et administration de programmes	2 524 935	1 485 318
TVH non réclamable	10 336	34 213
Charges totales	5 108 418	1 519 531
Excédent (insuffisance) des produits sur les charges	236 678 $	(40 628)$

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État des flux de trésorerie

Pour l'exercice terminé le 31 mars	2025	2024
Flux de trésorerie liés aux activités de fonctionnement		
Excédent (insuffisance) des produits sur les charges	236 678 $	(40 628)$
Variations des éléments hors caisse du fonds de roulement:		
Comptes à recevoir	(117 410)	(140 823)
Autres créances	46 200	(22 422)
Frais payés d'avance	(74 029)	(15 830)
Créditeurs et frais courus	154 693	(83 061)
Subventions et adhésions reportées	1 485 534	1 313 273
Avances de projets	3 994 276	-
Subventions à payer – récipiendaires finaux	952 266	-
Subventions à payer – remboursements	1 303 926	-
	(6 418)	1 010 509
Flux de trésorerie liés aux activités d'investissement		
Changement au dû aux membres fondateurs	2 500	(37 500)
(Diminution) augmentation nette de la trésorerie	(3 918)	1 019 210
Encaisse, début de l'exercice	1 520 299	501 089
Encaisse, fin de l'exercice	1 516 381 $	1 520 299 $

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
Notes complémentaires

31 mars 2025

1. Méthodes comptables

Statut et objectif de l'organisme	Consortium national pour la cybersécurité (le « consortium ») est un organisme sans but lucratif constitué sans capital-actions en vertu de la Loi canadienne sur les organisations sans but lucratif le 3 mars 2020, en tant qu'organisation fondée par les membres avec une entente entre Innovation, Sciences et Développement économique Canada (ISDE) et le Consortium national pour la cybersécurité. Le consortium est un organisme sans but lucratif au sens de la Loi de l'impôt sur le revenu et, à ce titre, il est exonéré d'impôt. Le mandat du Consortium est de faire progresser l'écosystème de la cybersécurité du Canada par la recherche et le développement, la commercialisation et la formation.
Référentiel comptable	Le consortium applique les Normes comptables canadiennes pour les organismes sans but lucratif.
Utilisation d'estimations	La préparation des états financiers exige que la direction procède à des estimations et pose des hypothèses qui ont une incidence sur les montants présentés au titre des actifs et des passifs et sur les montants comptabilisés au titre des produits et des charges pour l'exercice visé.
Comptabilisation des produits	Le consortium applique la méthode du report pour comptabiliser les apports. Les apports affectés sont comptabilisés à titre de produits de l'exercice au cours duquel les charges connexes sont engagées. Les apports non affectés sont comptabilisés à titre de produits lorsqu'ils sont reçus ou à recevoir si le montant à recevoir peut faire l'objet d'une estimation raisonnable et que sa réception est raisonnablement assurée. Les adhésions sont comptabilisées à titre de produits au prorata dans l'exercice auquel elles se rapportent.

1. Méthodes comptables (suite)

Instruments financiers	Les instruments financiers dans des conditions de pleine concurrence sont comptabilisés à la juste valeur lors de la comptabilisation initiale. Les instruments financiers contractés entre apparentés cotés sur un marché actif ou pour lesquels des données d'entrée importantes pour la détermination de la juste valeur de l'instrument sont observables ou des contrats dérivés existent sont comptabilisés à la juste valeur lors de la comptabilisation initiale. Tous les autres instruments financiers contractés entre apparentés sont comptabilisés au coût lors de la comptabilisation initiale. Les actifs financiers font l'objet d'un test de dépréciation lorsqu'il y a des indicateurs d'une perte de valeur. Lorsqu'un changement important dans le calendrier ou les flux de trésorerie futurs de l'actif financier est identifié, la valeur comptable de cet actif est réduite et le montant est constaté à titre de dépréciation dans le résultat net. La moins-value déjà comptabilisée peut faire l'objet d'une reprise dans la mesure de l'amélioration, pourvu qu'elle ne dépasse pas le montant qui aurait été constaté à la date de la reprise si la moins-value n'avait jamais été comptabilisée, et le montant de la reprise de valeur est comptabilisé en résultat net.

2. Créditeurs et frais courus

Le poste créditeurs et frais courus comprend des sommes à remettre à l'État de 49 344 $ (2024 - nul).

3. Subventions et adhésions reportées

	2025	2024
Subventions d'ISED reportées	2 740 844 $	1 310 827 $
Adhésions reportées	258 682	203 165
Solde, à la fin de l'exercice	2 999 526 $	1 513 992 $

	2025	2024
Solde, au début de l'exercice	1 513 992 $	200 719 $
Plus: subventions d'ISED reçues pendant l'année	6 435 345	2 756 146
Plus: adhésions reçues pendant l'année	367 880	236 750
Moins: subventions d'ISED constatées à titre de produits de l'exercice	(5 010 800)	(1 445 318)
Moins: adhésions constatées à titre de produits de l'exercice	(309 862)	(33 585)
Solde, à la fin de l'exercice	2 999 526 $	1 513 992 $

4. Dépendance économique

Le consortium a reçu 94% (2024 - 98%) de ses produits d'ISED. Si ce financement ne continue pas ou si le consortium ne peut pas le remplacer, le consortium ne pourrait pas continuer ses opérations au niveau actuel.

5. Instruments financiers

Risque de liquidité
Le risque de liquidité est le risque que le Consortium puisse rencontrer des difficultés à respecter ses obligations financières à leur échéance. Cela inclut le risque que, en raison de contraintes de liquidité opérationnelle, le Consortium n'ait pas suffisamment de fonds pour régler les transactions à leurs dates d'échéance, soit contraint de vendre des actifs financiers à des prix défavorables, ou soit incapable de récupérer la pleine valeur des actifs financiers. Le Consortium est principalement exposé au risque de liquidité par ses créditeurs et charges à payer. Le risque n'a pas changé depuis l'année dernière

Risque de crédit
Le consortium est esposé au risque de crédit puisque tous ses comptes bancaires sont détenus auprès d'une seule institution financière. Il n'y a pas eu de variation dans le risque comparativement à l'année précédente.

National Cybersecurity Consortium
Consortium national pour la cybersécurité
Financial Statements
For the year ended March 31, 2025

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, 2025, 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, 2025, 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.

BDO Canada LLP

Chartered Professional Accountants
Ottawa, Ontario
June 26, 2025

National Cybersecurity Consortium
Statement of Financial Position

March 31	2025	2024
Assets		
Current		
Cash	$ 1,516,381	$ 1,520,299
Accounts receivable	191,492	140,823
Other receivables	76,710	46,200
Prepaid expenses	100,375	26,346
Project advances	3,994,276	-
	$ 5,879,234	$ 1,733,668
Liabilities and Net Assets (Deficiency)		
Current		
Accounts payable and accrued liabilities (Note 2)	$ 292,149	$ 127,487
Grants payable – reimbursements	1,303,926	-
Grants payable – ultimate recipients	952,266	-
Deferred grants and memberships (Note 3)	2,999,526	1,513,992
Due to founding members	115,000	112,500
	$ 5,662,867	1,753,979
Net Assets (Deficiency)		
Unrestricted	216,367	(20,311)
	$ 5,879,234	$ 1,733,668

On behalf of the Board:

Signed by:
Charmaine B. Dean
41D0855C03A4474...
Director

Signed by:
David MaGee
9C036B809005435...
Director

The accompanying notes are an integral part of these financial statements.

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

For the year ended March 31	2025	2024
Balance, beginning of the year	$ (20,311)	$ 20,317
Excess (deficiency) of revenues over expenses	236,678	(40,628)
Balance, end of the year	$ 216,367	$ (20,311)

The accompanying notes are an integral part of these financial statements.

National Cybersecurity Consortium
Statement of Operations

For the year ended March 31	2025	2024
Revenues		
Grants (Note 2)	$ 5,010,800	$ 1,445,318
Memberships (Note 2)	309,862	33,585
Interest and other income	24,434	-
	5,345,096	1,478,903
Expenses		
Programs	2,573,147	-
Program development, delivery, and administration	2,524,935	1,485,318
Unclaimable HST	10,336	34,213
	5,108,418	1,519,531
Excess (deficiency) of revenues over expenses	$ 236,678	$ (40,628)

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	2025	2024
Cash flows from operating activities		
Excess (deficiency) of revenues over expenses	$ 236,678	$ (40,628)
Changes in non-cash working capital:		
Accounts receivable	(117,410)	(140,823)
Other receivables	46,200	(22,422)
Prepaid expenses	(74,029)	(15,831)
Accounts payable and accrued liabilities	154,693	(36,859)
Deferred grants and memberships	1,485,534	1,313,273
Project advances	3,994,276	-
Grants payable – ultimate recipients	952,266	-
Grants payable – reimbursements	1,303,926	-
	(6,418)	1,056,710
Cash flows from financing activities		
Change in due to founding members	2,500	(37,500)
Net (decrease) increase in cash	(3,918)	1,019,210
Cash, beginning of the year	1,520,299	501,089
Cash, end of the year	$ 1,516,381	$ 1,520,299

The accompanying notes are an integral part of these financial statements.

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.

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 $49,344 (2024 - nil).

3. Deferred Grants and Memberships

	2025	2024
Deferred ISED grants	$ 2,740,844	$ 1,310,827
Deferred memberships	258,682	203,165
Balance, end of year	$ 2,999,526	$ 1,513,992

	2025	2024
Balance, beginning of year	$ 1,513,992	$ 200,719
Plus: ISED grants received in the current year	6,435,345	2,756,146
Plus: Memberships received in the current year	367,880	236,750
Less: ISED grants recognized as revenue in the year	(5,010,800)	(1,445,318)
Less: Memberships recognized as revenue in the year	(309,862)	(33,585)
Balance, end of year	$ 2,999,526	$ 1,513,992

4. Economic Dependence

The Consortium received 94% (2024 - 98%) 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 and accrued liabilities. The risk has not changed since last year.

Credit risk

The Consortium's is exposed to the credit risk arising from all of its bank accounts held at a single financial institution. The risk has not changed since last year.