Innovation, Sciences et Développement économique Canada
Innovation, Science and Economic Development Canada
Canada

RÉSEAU D'INNOVATION POUR LA CYBERSÉCURITÉ

Cette publication est également offerte en ligne : https://www.ic.gc.ca/eic/site/149.nsf/fr/h_00000.html

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication : www.ic.gc.ca/demande-publication ou communiquer avec :

Centre de services aux citoyens d'ISDE
Innovation, Sciences et Développement économique Canada
Édifice C.D. Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5
Canada

Téléphone (sans frais au Canada): 1-800-328-6189
Téléphone (international): 613-954-5031
ATS (pour les personnes malentendantes): 1-866-694-8389

Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)

Courriel: ISDE@ised-isde.gc.ca

Autorisation de reproduction

N° de catalogue Iu37-30/2021F-PDF
ISBN 978-0-660-37905-0

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

Also available in English under the title *Cyber Security Innovation Network Program*.

Table des matières

1. Introduction au Réseau d'innovation pour la cybersécurité

1.1 Contexte

Dans son budget de 2019, le gouvernement a annoncé un investissement de 80 millions de dollars sur quatre ans pour appuyer au moins trois centres d'expertise canadiens en matière de cybersécurité au Canada, qui sont affiliés à des établissements d'enseignement postsecondaire. Le programme du Réseau d'innovation pour la cybersécurité a pour but de financer un réseau national pour la cybersécurité qui sera dirigé par des centres d'expertise canadiens en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire (au moins trois centres d'expertises participants), en collaboration avec le secteur privé et d'autres partenaires. Le Réseau se voudra un réseau pancanadien qui visera à appuyer la recherche et développement (R-D), à accroître la commercialisation et à soutenir davantage le perfectionnement et le développement de talents qualifiés dans le domaine de la cybersécurité partout au Canada.

Innovation, Sciences et Développement économique Canada (ISDE) cherche à conclure une entente de contribution non remboursable de quatre ans avec un demandeur retenu pour former le Réseau d'innovation pour la cybersécurité. La valeur de l'entente de contribution totalisera au plus 80 millions de dollars sur quatre ans (de 2021-2022 à 2024-2025).

Le présent guide fournit des renseignements sur les objectifs du programme, les critères d'admissibilité et d'évaluation, les résultats escomptés, ainsi que de l'information détaillée sur la façon de présenter une demande.

1.2 Vision, mission et objectifs du Réseau d'innovation pour la cybersécurité

Vision : Appuyer la création d'un réseau national visant à favoriser la croissance de l'écosystème de la cybersécurité au Canada par l'entremise d'une collaboration entre l'industrie et le milieu universitaire.

Mission : Le Réseau d'innovation pour la cybersécurité visera à appuyer et à étendre la recherche et le développement, à accroître la commercialisation et à soutenir davantage le perfectionnement et le développement de talents qualifiés dans le domaine de la cybersécurité.

Objectifs :

- Le réseau appuiera la recherche et le développement dans le domaine de la cybersécurité en favorisant la collaboration entre les établissements d'enseignement postsecondaire au Canada, le secteur privé et d'autres partenaires en vue d'accélérer l'élaboration de produits et/ou de services de cybersécurité novateurs;
- Le réseau cherchera à accélérer la commercialisation des produits, des services et/ou des processus de cybersécurité qui sont mis sur le marché;
- Le réseau visera à diversifier, à approfondir et à élargir la réserve de talents du Canada dans le domaine de la cybersécurité, dont le recrutement et le maintien en poste du corps professoral, de formateurs et d'instructeurs. Il visera également à fournir davantage de ressources pour permettre l'élaboration de programmes d'études, la formation, la

requalification et le perfectionnement de la main-d'œuvre en matière de cybersécurité au moyen d'initiatives conçues et offertes en collaboration avec les partenaires de l'industrie.

2. Exigences du programme

2.1 Critères d'admissibilité

Pour être admissibles au programme du Réseau d'innovation pour la cybersécurité, les demandeurs doivent répondre à tous les critères suivants dans leur proposition :

- être établis comme un réseau qui sera dirigé par au moins trois centres d'expertise canadiens en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire;
  - Un centre se définit comme une organisation affiliée à un établissement d'enseignement postsecondaire canadien reconnu qui favorise la croissance de l'écosystème d'innovation en matière de cybersécurité.

- être constitués en vertu des lois fédérales comme une organisation à but non lucratif aux termes de la *Loi canadienne sur les organisations à but non lucratif* (l'incorporation n'est pas requise au moment de l'application);

- être représentatifs de la diversité de l'écosystème du Canada en matière de cybersécurité. ISDE s'attend à ce que les catégories de partenaires suivantes, notamment, soient représentées dans la proposition de réseau :
  - centres d'expertise en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire (autres que les centres qui se présentent à titre de demandeurs);
  - secteur privé (y compris des petites et moyennes entreprises (PME) et des grandes entreprises);
  - établissements d'enseignement postsecondaire canadiens (p. ex., centres de recherche, universités, collèges, polytechniques);
  - organisations à but non lucratif (p. ex., associations industrielles, incubateurs et accélérateurs d'entreprises, organismes de perfectionnement de compétences, etc.);
  - gouvernements provinciaux et territoriaux/administrations municipales.

- comprendre des engagements provenant d'une combinaison de partenaires visant à égaler les fonds nécessaires dans le cadre du programme de Réseau d'innovation pour la cybersécurité selon un ratio de 1:1 (pour de plus amples renseignements, consultez la section 2.9 : Exigences de financement de contrepartie);

- être présents à l'échelle du Canada, c'est-à-dire qu'ils comprennent des centres d'expertise en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire et des partenaires de toutes les régions du Canada (l'Ouest et le Nord du Canada, le centre [avec des représentants de l'Ontario et du Québec] et le Canada atlantique);

- faire preuve d'une vision nationale pour permettre au réseau de faire avancer la recherche et développement, la commercialisation et les compétences en matière de cybersécurité, ainsi que les activités de perfectionnement et de développement de talents qui reflètent les secteurs ayant des besoins et des spécialisations en matière de cybersécurité partout au Canada.

Modèle du réseau

Bénéficiaire principal

Après la signature de l'entente de contribution, le demandeur sera désigné comme le « bénéficiaire principal ». Le bénéficiaire principal doit être constitué comme une organisation à but non lucratif en vertu de la *Loi canadienne sur les organisations à but non lucratif*, avant que l'entente de contribution ne soit signée. Le bénéficiaire principal sera l'organisme chargé de la mise en œuvre de l'orientation stratégique du réseau afin d'atteindre les objectifs du programme du Réseau d'innovation pour la cybersécurité. Il sera aussi en charge de l'administration et de la réaffectation de la contribution fédérale.

Le bénéficiaire principal devra gérer ses propres opérations. ISDE n'assumera pas un rôle opérationnel dans la mise en œuvre des activités ou dans la gestion des relations entre les organisations faisant partie du réseau proposé.

Bénéficiaires ultimes

Le bénéficiaire principal peut verser des fonds à des bénéficiaires ultimes qui exécuteront les activités décrites dans l'entente de contribution (voir la section 2.3 portant sur les activités admissibles pour de plus amples renseignements). ISDE s'attend à ce que le bénéficiaire principal signe des ententes de financement exécutoires avec les bénéficiaires ultimes et qu'il surveille leur conformité aux modalités, conditions et obligations énoncées dans l'entente de contribution afin de suivre les progrès et de veiller à l'utilisation responsable des fonds.

À titre d'exemples, les bénéficiaires ultimes dans le réseau peuvent être des organisations qui :

- contribueront à fournir du financement de contrepartie et qui réaliseront des activités liées à un projet;
- exécuteront des activités liées à un projet sans fournir de financement de contrepartie (p. ex., les bénéficiaires ultimes pourraient être choisis à l'issue d'un appel de propositions et recevoir uniquement du financement du réseau).

Les types d'organisations suivantes peuvent devenir des bénéficiaires ultimes :

- des centres d'expertise en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire (autres que les centres qui se présentent à titre de demandeurs);
- des entités du secteur privé (y compris des petites et moyennes entreprises et des grandes entreprises);

- des établissements d'enseignement postsecondaire canadiens (p. ex., centres de recherche, universités, collèges, polytechniques);
- des organisations à but non lucratif (p. ex., associations industrielles, incubateurs et accélérateurs d'entreprises, organismes de perfectionnement de compétences, etc.).

2.2 Structure de gouvernance et gestion

Le bénéficiaire principal doit se doter de structures administratives et de gouvernance pour appuyer les activités du réseau. Les demandeurs devront démontrer comment ils comptent mettre en place les structures de gouvernance suivantes, qui constituent des exigences.

Conseil d'administration

Étant donné qu'une entité fédérale à but non lucratif sera créée, le réseau doit mettre sur pied un conseil d'administration qui assumera la responsabilité globale de la gouvernance et de la gestion du Réseau d'innovation pour la cybersécurité. Le conseil d'administration sera chargé de la gestion du réseau, de l'orientation stratégique et de la responsabilité financière, ainsi que de l'exécution du plan organisationnel annuel du réseau et de l'approbation du rapport annuel et des états financiers vérifiés.

La participation du secteur privé (y compris des PME et de plus grandes entreprises) au sein du conseil d'administration et de la structure de gouvernance du réseau est attendue. La participation devra être diversifiée, inclusive, paritaire et pancanadienne. La composition du conseil d'administration permanent devra viser à atteindre une représentation paritaire des sexes de 50 p. 100 et une participation de 30 p. 100 d'autres groupes sous-représentés (voir le cadre de l'équité, de la diversité et de l'inclusion de la section 2.8 Cadre de l'équité, de la diversité et de l'inclusion pour obtenir de plus amples renseignements).

Principaux postes de direction

	Poste	Description
1.	**Directeur général**	Le réseau devra nommer un directeur général qui relèvera du conseil d'administration. Le directeur général sera chargé des opérations du réseau.
2.	**Directeur de la sécurité de l'information**	Le réseau devra nommer un directeur de la sécurité de l'information qui sera chargé de diriger la mise en œuvre de la stratégie relative à la gestion des données et du plan de cybersécurité du réseau. Consultez le Plan de cybersécurité à la section 2.4 et la Stratégie relative à la gestion des données à la section 2.5 pour obtenir des renseignements détaillés.
3.	**Directeur financier**	Le réseau devra nommer un directeur financier qui sera chargé de la gestion des finances du réseau.

Personnel du réseau

Le réseau doit embaucher des employés chargés de l'exécution des activités opérationnelles, ce qui comprend, sans toutefois s'y limiter, la redistribution des fonds du programme, les projets internes et les partenariats. Les employés des opérations assumeront également la responsabilité de faire la liaison avec ISDE et de préparer les documents exigés aux termes de l'entente de contribution (voir la section 5. Encadrement et surveillance pour obtenir de plus amples renseignements).

Le réseau sera encouragé à créer d'autres postes clés afin de soutenir l'exécution des opérations du réseau. Les postes pourraient comprendre les suivants :

- un directeur des ressources humaines;
- un directeur de l'équité, de la diversité et de l'inclusion (EDI);
- un gestionnaire de la propriété intellectuelle (PI);
- un gestionnaire du développement des affaires et des partenariats.

Comités

En plus du conseil d'administration, des cadres et du personnel opérationnel, le réseau proposé devra mettre sur pied des comités pertinents pour faire progresser les activités du réseau. À tout le moins, le bénéficiaire principal devra créer un comité pour la sélection des projets (voir la section 2.3 Activités admissibles pour obtenir de plus amples renseignements).

Cadre sur les conflits d'intérêts

L'atteinte des objectifs du Réseau d'innovation pour la cybersécurité nécessite divers types d'interactions entre les participants du réseau, dont certaines pourraient placer des personnes en situation de conflit d'intérêts potentiel, apparent ou réel. Le bénéficiaire principal doit élaborer un cadre sur les conflits d'intérêts à l'intention des administrateurs, des cadres, des employés et des membres des comités qui aura pour but d'empêcher des conflits d'intérêts réels ou perçus. Le cadre devra comprendre un processus pour la divulgation et un mécanisme pour la gestion des conflits.

Structure d'adhésion au réseau

Le Réseau d'innovation pour la cybersécurité devra mettre en place une structure d'adhésion pour officialiser la participation provenant de l'écosystème (autre que les bénéficiaires ultimes qui concluront des ententes de contribution avec le bénéficiaire principal) et fournira des renseignements détaillés sur la façon dont les participants profiteront des activités du réseau. La structure d'adhésion doit clarifier les modalités régissant l'adhésion des membres (y compris la cotisation, s'il y a lieu). 'L'adhésion au réseau peut évoluer au fil du temps et le modèle de participation proposé doit être inclusif pour s'assurer que toutes les parties intéressées puissent se joindre au réseau et bénéficier de ses activités. La structure d'adhésion finale figurera dans l'entente de contribution.

2.3 Activités admissibles

Le Réseau d'innovation pour la cybersécurité devrait mener des activités visant à appuyer la recherche et développement, à accroître la commercialisation et à soutenir le perfectionnement de talents qualifiés. Les activités de recherche, de développement et de commercialisation peuvent couvrir les niveaux de maturité technologique (NMT) de 1 à 9 et pourraient comprendre ce qui suit (consultez l'Annexe A – Échelle des niveaux de maturité technologique pour obtenir de plus amples renseignements au sujet des NMT) :

La recherche et développement de technologie collaborative en matière de cybersécurité, notamment :

- le design conceptuel, la validation de concept, le développement de prototypes, la création de propriété intellectuelle, les essais technologiques ou de produits et les activités de mobilisation du savoir;

- le développement de nouveaux produits, services et/ou procédés.

La commercialisation de produits et services novateurs en matière de cybersécurité, notamment :

- les activités liées à l'exploitation et à la conservation de la propriété intellectuelle;
- des services de développement des affaires à l'intention des entreprises afin de faciliter l'accès à de nouveaux clients et d'étendre les marchés, ce qui pourrait comprendre des études de marché et des services consultatifs, en plus d'autres services corporatifs (p. ex., jumeler des entreprises en démarrage avec des partenaires stratégiques, organiser des journées de présentation d'argumentaires éclairs, mener des activités de marketing, etc.).

Le développement d'approches nationales novatrices pour remédier aux lacunes en matière de compétences et de main-d'œuvre au Canada et pour permettre aux entreprises canadiennes de s'attaquer aux défis liés à la cybersécurité, notamment :

- la détermination et la communication des besoins de l'industrie en matière de compétences (p. ex., évaluation des besoins présents et futurs de l'industrie en matière de main-d'œuvre, sensibilisation de divers intervenants concernant les besoins de l'industrie en matière de compétences, analyses environnementales, ateliers, etc.);

- des modules de formation (y compris des solutions relatives au perfectionnement et à la requalification);

- le développement et la promotion de parcours académiques pour des études définies dans le domaine de la cybersécurité; le développement de programmes scolaires, et un soutien en enseignement pour exécuter le programme scolaire;

- l'encadrement ou le mentorat;

- les programmes d'enseignement coopératif et/ou d'autres types d'apprentissage en milieu de travail (p. ex., formations d'apprenti, stages, travaux pratiques, etc.) et des solutions pour aider les entreprises à assurer la transition des étudiants vers le marché du travail.

Les activités énumérées ci-dessus pourraient être exécutées par les bénéficiaires ultimes et devraient comprendre un haut niveau de collaboration en vue de renforcer les liens entre les partenaires.

Le bénéficiaire principal sera chargé des activités liées à la coordination, à la supervision et à la responsabilité des activités du réseau dans ces trois domaines. Ces activités peuvent comprendre, notamment :

- l'organisation d'événements de réseautage (ces événements ne comprennent pas les réunions de nature générale et qui font partie des exigences opérationnelles récurrentes);
- l'organisation de conférences et d'ateliers à l'appui d'activités de recherche et de développement menées en collaboration;
- l'exploitation des bureaux du réseau (sièges sociaux et bureaux régionaux);
- la sélection et la gestion de projets;
- autres activités pouvant être considérées comme admissibles et assujetties à l'approbation du programme du Réseau d'innovation pour la cybersécurité.

Projets planifiés et prêts à être exécutés

Pour s'assurer d'une mise en œuvre en temps opportun des activités du réseau, les demandeurs devront fournir dans leur proposition des renseignements détaillés au sujet des activités qui ont déjà été identifiées et qui pourraient être réalisées dans la première année des opérations du réseau, y compris la confirmation de financement de contrepartie pour ces projets.

Critères et processus de sélection des projets du réseau

Un bénéficiaire principal peut lancer régulièrement des appels de propositions pour des projets ayant trait aux activités ciblées décrites ci-dessus. Un bénéficiaire principal devra mettre en œuvre un cadre d'évaluation pour la sélection et l'approbation des projets. Les demandeurs devront fournir des renseignements détaillés au sujet de leurs plans, y compris les échéanciers et les critères de sélection des projets du réseau. Ces renseignements figureront dans l'entente de contribution.

La sélection des projets doit se faire au moyen de processus ouverts, équitables, transparents et dirigés par des experts pour s'assurer de respecter les normes d'évaluation fondées sur le mérite et de fournir une contribution utile à l'écosystème selon les buts du réseau.

Les critères de sélection des projets comprendront au minimum ce qui suit :

- un engagement de financement;
- l'échéancier du projet;
- les évaluations des avantages potentiels économiques, sur le plan de l'innovation et pour le grand public;

- la faisabilité technique d'un projet;
- les domaines de spécialisation en matière de cybersécurité;
- le potentiel de commercialisation au Canada (y compris la propriété intellectuelle);
- la participation du secteur privé et d'autres partenaires qui est représentative de la diversité d'organisations au sein de l'écosystème de la cybersécurité au Canada;
- les possibilités de collaboration et de synergie entre les projets;
- la représentation régionale;
- la capacité financière des bénéficiaires ultimes d'exécuter les projets;
- la contribution du projet à l'atteinte des objectifs du réseau pour appuyer la R-D, accroître la commercialisation et soutenir le perfectionnement de talents qualifiés dans le domaine de la cybersécurité;
- les retombées du projet qui renforcent et favorisent la viabilité du réseau.

Le bénéficiaire principal devra former un comité chargé de la sélection des projets qui satisfait aux critères suivants :

- être constitué d'un tiers (1/3) de membres indépendants;
  - Les membres indépendants sont des particuliers qui ne bénéficieront pas directement des activités de l'organisation et qui n'ont aucun lien matériel avec le réseau (et le bénéficiaire principal) pouvant directement ou indirectement, en réalité ou en apparence, nuire à leur capacité de réfléchir et d'agir de manière indépendante dans l'intérêt du réseau.
- être représentatif de l'industrie de la cybersécurité, de la recherche et de l'écosystème de compétences;
- être pancanadien;
- respecter les principes d'équité, de diversité et d'inclusion.

2.3.1 Coûts admissibles

La contribution du programme versée à un bénéficiaire admissible ne dépassera pas 50 p. 100 du total des coûts admissibles, sauf si les bénéficiaires admissibles sont des établissements d'enseignement postsecondaire, lequel cas la contribution pourrait atteindre 100 p. 100 des coûts admissibles.

Coûts administratifs et opérationnels

Les coûts administratifs et opérationnels admissibles comprennent les coûts engagés par le bénéficiaire principal pour soutenir les opérations courantes du réseau et appuyer la concrétisation de son mandat.

Coûts liés aux projets

Les coûts admissibles liés aux projets ont trait aux activités menées par les bénéficiaires ultimes pour exécuter les activités du Réseau d'innovation pour la cybersécurité. De telles dépenses pourraient comprendre :

a) le recrutement et le maintien en poste de professeurs, d'étudiants diplômés, de candidats postdoctoraux, de chercheurs, d'ingénieurs de soutien et de personnel administratif;

b) les coûts directs de la recherche, comme l'accès aux installations et à l'équipement, les biens et le matériel, les salaires et les indemnités;
c) les coûts liés à la mobilisation du savoir, à l'échange et à l'exploitation de la technologie (p. ex., développement de prototypes, études de marché, propriété intellectuelle liée à la recherche des centres et élaboration de politiques);
d) jusqu'à 20 p. 100 des fonds peuvent être utilisés pour l'équipement et l'infrastructure nécessaires à la recherche, au développement et à la formation des étudiants et des chercheurs.

Les coûts admissibles pour les activités entreprises par le bénéficiaire principal et les bénéficiaires finaux sont catégorisés comme suit :

a) Coûts salariaux directs;
b) Sous-traitants et consultants;
c) Équipement;
d) Coûts directs;
e) Coûts de déplacement et coûts des activités de sensibilisation;
f) Coûts indirects (frais généraux).

Les plafonds des coûts indirects (frais généraux) de 55 p. 100 du total des coûts directs admissibles de la main-d'œuvre et d'au plus 15 p. 100 s'appliqueront au bénéficiaire principal et aux bénéficiaires ultimes.

Les coûts engagés à l'extérieur du Canada ne peuvent représenter plus de 10 p. 100 du total des coûts admissibles déclarés.

Au cas par cas, le ministre pourrait envisager le remboursement rétroactif de coûts admissibles engagés par un bénéficiaire principal avant la signature de l'entente de contribution, mais pas avant la date d'approbation de la demande. Les coûts admissibles à un remboursement rétroactif ne doivent pas dépasser 20 p. 100 du total des coûts admissibles. Le ministre ne sera pas tenu de rembourser les coûts engagés si une demande est rejetée ou n'est pas approuvée aux fins de financement.

2.3.2 Coûts inadmissibles

Certains coûts ne sont pas admissibles à un remboursement, indépendamment du fait qu'ils ont été engagés de façon raisonnable et appropriée dans le cadre d'un projet approuvé.

Les coûts inadmissibles comprendront les suivants :

a) un soutien direct pour la certification professionnelle;
b) toute forme d'intérêt payé ou payable sur le capital investi, les obligations, les débentures, les prêts bancaires ou autres, y compris les escomptes à l'émission d'obligations et les frais de financement connexes; la partie des intérêts du coût de location qui est attribuable au coût d'emprunt, peu importe le type de bail;

c) les frais juridiques et les honoraires comptables et d'experts-conseils en lien avec la réorganisation financière (y compris la création de nouvelles organisations à but non lucratif), des enjeux de sécurité, des enjeux de capital-actions, l'obtention de licences, la création et la gestion d'ententes avec des bénéficiaires ultimes et les poursuites contre le ministre. De tels coûts peuvent être admissibles s'ils sont liés à l'obtention de brevets ou d'une autre protection légale pour la propriété intellectuelle du projet;
d) les pertes subies en raison de mauvais investissements, de mauvaises créances et des frais de recouvrement;
e) les pertes subies sur d'autres contrats ou projets;
f) les impôts sur le revenu, fédéral et provincial, les taxes sur les produits et services, les taxes ou surtaxes sur les profits excédentaires, ou les dépenses spéciales associées à ces impôts;
g) les provisions pour risques;
h) les primes relatives aux assurances-vie des cadres ou des administrateurs lorsque le produit de l'assurance est versé au bénéficiaire principal et/ou aux bénéficiaires ultimes;
i) l'amortissement de la plus-value non réalisée des biens;
j) l'amortissement des immobilisations payées par le ministre;
k) les amendes et les dommages-intérêts;
l) la rémunération déraisonnable des cadres et des employés;
m) les frais d'élaboration et d'amélioration de produits qui n'ont pas été engagés dans le cadre du projet;
n) les frais de publicité, sauf les frais raisonnables de publicité de nature industrielle ou institutionnelle versés pour les annonces placées dans des publications spécialisées, techniques ou professionnelles en vue de fournir de l'information à l'industrie ou à l'institution;
o) les frais de divertissement qui comprennent, sans toutefois s'y limiter, les services de traiteur, les boissons alcoolisées et les dépenses non liées aux voyages;
p) les dons;
q) les cotisations et autres frais, sauf ceux des associations professionnelles et commerciales ordinaires;
r) les frais extraordinaires ou anormalement élevés d'experts-conseils concernant des questions techniques, administratives ou de comptabilité, à moins d'avoir obtenu l'approbation du ministre;
s) les frais de vente et de commercialisation liés aux biens, aux services ou aux deux acquis en vertu de l'entente de contribution;
t) les coûts en nature; Les coûts en nature ne peuvent être remboursés par une contribution fédérale, mais peuvent être indiqués pour respecter les exigences de financement de contrepartie du programme. Consultez la section 2.9 Exigences relatives au financement de contrepartie pour obtenir de plus amples renseignements sur les exigences relatives au financement de contrepartie.

2.4 Plan de cybersécurité

Le bénéficiaire principal devra fournir à ISDE un plan de cybersécurité aux fins d'approbation avant son inclusion dans l'entente de contribution. Dans le cadre du processus de demande, les demandeurs devront démontrer comment ils comptent s'assurer de la cyber résilience et proposer des stratégies pour identifier les incidents potentiels en matière de cybersécurité, s'en protéger, les détecter, y réagir et s'en remettre.

Le bénéficiaire principal sera tenu de faire ce qui suit :

- déterminer les risques et les vulnérabilités en matière de cybersécurité associés aux opérations et aux activités du réseau;
- démontrer comment il tentera de mettre en œuvre l'approche En route vers la sécurité d'entreprise mise au point par le Centre canadien pour la cybersécurité (CCC), à commencer par les contrôles de cybersécurité de base pour les petites et moyennes organisations;
- utiliser l'Outil canadien de cybersécurité (OCC), un outil virtuel d'auto-évaluation conçu par Sécurité publique Canada (SP) en collaboration avec le Centre de la sécurité des télécommunications (CST) et le Centre canadien pour la cybersécurité qui donne au participant un aperçu de la résilience opérationnelle et de la situation en matière de cybersécurité de son organisation. Les résultats de l'auto-évaluation aideront le CCC à fournir une orientation et des outils au bénéficiaire principal pour l'aider dans l'élaboration d'un plan de cybersécurité qui sera inclus dans l'entente de contribution;
- avant de conclure une entente de contribution, évaluer les plans de cybersécurité des bénéficiaires ultimes et la capacité de ces derniers à les mettre en œuvre;
- s'assurer que les bénéficiaires ultimes et leurs fournisseurs de services respectent les normes les plus élevées en matière de sécurité et d'intégrité dans leurs activités et équipement et ont de solides réputations et antécédents au Canada;
- signaler, périodiquement et au besoin, les incidents de cybersécurité et les plans d'intervention du réseau et/ou des bénéficiaires ultimes.

Les bénéficiaires ultimes seront tenus de faire ce qui suit :

- soumettre aux fins d'examen un plan de cybersécurité au bénéficiaire principal; le plan doit comprendre de l'information au sujet de sa situation en matière de cybersécurité et de la façon dont il mettra en œuvre les contrôles de cybersécurité de base pour les petites et moyennes organisations, mis au point par le Centre canadien pour la cybersécurité.

CyberSécuritaire Canada

Les bénéficiaires ultimes sont encouragés à présenter une demande de certification auprès de CyberSécuritaire Canada. CyberSécuritaire Canada est un programme de certification en cybersécurité du gouvernement fédéral qui vise à aider les PME canadiennes à répondre aux exigences de base en matière de cybersécurité, à accroître la confiance des consommateurs dans l'économie numérique, à promouvoir les normes internationales et à mieux positionner les PME pour qu'elles soient concurrentielles à l'échelle mondiale. La certification exige la mise en œuvre des contrôles de sécurité de base mis au point par le Centre canadien pour la cybersécurité. Le sceau de certification de CyberSécuritaire Canada confère une reconnaissance officielle du gouvernement fédéral attestant de la conformité de l'entité certifiée aux contrôles de sécurité de base.

Remarque sur la prochaine norme nationale en matière de cybersécurité

En décembre 2019, le Conseil canadien des normes (CCN) a entamé sa collaboration avec le Conseil stratégique des DPI afin d'élaborer une norme canadienne pour le programme de certification CyberSécuritaire Canada. La première édition de la nouvelle norme portera sur les contrôles de sécurité de base. Les consultations publiques à l'appui du standard se sont déroulées à l'hiver 2021 et la norme devrait être publiée avant la fin de 2021. La norme, qui vise à éviter l'imposition d'un lourd fardeau, se veut facilement accessible, abordable, efficace, nationale et multisectorielle. Après la publication de la norme nationale, ISDE s'attend à ce que le Réseau d'innovation pour la cybersécurité l'intègre à ses activités et ses opérations.

2.5 Stratégie relative à la gestion des données

Le bénéficiaire principal doit démontrer comment il mettra en œuvre la stratégie relative à la gestion des données qui respectera les principes de la gestion et de la protection des données dans les opérations et les activités du réseau. Une stratégie relative à la gestion des données qui est efficace permettra d'assurer que l'information peut circuler facilement entre les participants du réseau afin de favoriser une collaboration efficace tout au long du cycle de vie des données.

Le bénéficiaire principal sera tenu de démontrer comment les composantes suivantes d'une stratégie relative à la gestion des données seront mises en œuvre et appliquées à ses activités et à celles des bénéficiaires ultimes.

La stratégie relative à la gestion des données du réseau devra comprendre à tout le moins :

1 - Des pratiques concernant la gestion des données :

- la gouvernance des données (p. ex., déterminer les rôles et responsabilités du bénéficiaire principal et des bénéficiaires ultimes; élaborer des politiques, des procédures et des lignes directrices pour s'assurer de la mise en œuvre des autorisations et des responsabilités associées aux données du réseau, dont les plans de relève, au besoin);
- la propriété des données (p. ex., s'assurer qu'il y a un détenteur clair des données qui seront recueillies, produites et échangées);
- la collecte des données (p. ex., des lignes directrices sur la façon dont les données existantes seront traitées et utilisées; les types de données qui seront recueillies, y compris les renseignements personnels s'il y a lieu; le format dans lequel les données seront recueillies; la façon dont les données recueillies seront structurées pour assurer la normalisation);
- les échanges de données (p. ex., des ententes sont en place pour veiller à l'interopérabilité et à l'accessibilité des parties autorisées);
- l'intégrité des données (p. ex., les formats de données structurés courants et les normes des technologies d'échange de données et les lignes directrices pour le stockage, la sauvegarde et la conservation des données sont en place);
- décrire toutes contraintes éthiques, juridiques et commerciales pouvant être imposées aux données du réseau.

2- La protection des données :

- Le réseau doit se conformer aux lois sur la protection des renseignements personnels et s'assurer que le bénéficiaire principal et les bénéficiaires ultimes ont l'autorisation légale de recueillir, d'utiliser ou de divulguer des renseignements personnels, de protéger ces renseignements et de respecter les droits et les obligations prévus dans les lois sur la protection des renseignements personnels.

2.6 Propriété intellectuelle

Le bénéficiaire principal et les bénéficiaires ultimes seront tenus de prendre les mesures appropriées pour protéger la propriété intellectuelle découlant d'activités appuyées par le réseau (PI soutenue par le réseau) afin d'optimiser les avantages économiques et sur le plan de l'innovation pour le Canada.

Le bénéficiaire principal devra fournir à ISDE, aux fins d'approbation, la stratégie du réseau en matière de propriété intellectuelle qui sera incluse dans l'entente de contribution et les ententes de financement des bénéficiaires ultimes. Le bénéficiaire principal et les bénéficiaires ultimes doivent agir d'une manière qui cadre avec la Stratégie du Réseau en matière de PI.

La stratégie du Réseau en matière de PI devra comprendre à tout le moins ce qui suit :

- une politique indiquant qui détient la propriété intellectuelle et l'accès des membres à cette dernière;
- des politiques claires sur le transfert technologique entre le milieu universitaire et l'industrie afin d'accroître la commercialisation de la recherche;
- des stratégies visant à encourager le plus possible la collaboration entre les intervenants canadiens et l'exploitation par ces derniers (p. ex., des approches concernant les licences relatives à la PI et aux produits qui en découlent);
- un plan pour aider les participants du réseau et les bénéficiaires ultimes à approfondir leurs connaissances et expertises en matière de PI (p. ex., offrir des cours, de la formation ou des ressources sur la PI, analyses panoramiques sur les brevets (patent landscaping), les poursuites liées aux brevets, études de liberté d'exploitation (freedom-to-operate), les possibilités d'attribution de licences à l'interne et à l'externe, etc.);
- un mécanisme ou un plan pour résoudre les conflits qui peuvent survenir entre les participants du réseau;
- un plan pour aider et encourager les participants du réseau et les bénéficiaires ultimes à obtenir des conseils juridiques indépendants et des services d'experts-conseils en matière de PI (p. ex., échanger de l'information au sujet des ressources disponibles, des cliniques juridiques en matière de PI, etc.).

De plus, dans le cadre de ses obligations, le bénéficiaire principal sera tenu de faire ce qui suit :

- évaluer les stratégies des bénéficiaires ultimes liées à la propriété intellectuelle et leur capacité à les mettre en œuvre avant de conclure une entente de contribution;
- évaluer les avantages attendus pour le Canada de la PI financée par le réseau.

Pour que les avantages de la propriété intellectuelle soient réalisés de manière appropriée, le Réseau d'innovation pour la cybersécurité devra concevoir ses activités de R-D et de commercialisation de manière à optimiser les avantages économiques, pour le grand public et sur le plan de l'innovation pour le Canada.

Le demandeur doit s'assurer que la propriété intellectuelle financée par le réseau continuera d'être détenue par des intérêts canadiens et que les bénéficiaires ultimes conserveront la capacité d'exploiter la PI financée par le réseau pour la durée du projet et un minimum de cinq ans après la fin du projet. La durée pourrait varier au cas par cas afin que le Canada profite des avantages et elle sera définie dans l'entente de contribution conclue entre le gouvernement du Canada et le bénéficiaire principal. Tout changement lié à la possession de la propriété intellectuelle ou à la capacité d'exploiter une PI financée par le réseau pendant la durée de l'entente nécessitera un consentement ministériel par écrit.

L'attribution de financement ne constituera pas à elle seule une raison suffisante pour que le gouvernement du Canada soit intéressé à détenir la PI découlant d'activités financées dans le cadre du programme du Réseau d'innovation pour la cybersécurité.

Considérations en matière de sécurité

Le bénéficiaire principal et les bénéficiaires ultimes devront exercer un processus de diligence raisonnable rigoureux et pertinent des risques liés à la sécurité que posent les activités de recherche du réseau et mettre en place des mesures en temps opportun pour atténuer ces risques de manière appropriée.

Le 24 mars 2021, le gouvernement du Canada a publié l'Énoncé de politique sur la sécurité de la recherche et a demandé aux membres du groupe de travail mixte du gouvernement du Canada et des universités d'élaborer des lignes directrices précises sur les risques afin d'intégrer les préoccupations de sécurité nationale dans l'évaluation et le financement des partenariats de recherche.

Ces lignes directrices aideront les chercheurs, les établissements de recherche et les bailleurs de fonds gouvernementaux à faire preuve de plus de diligence cohérente et axée sur le risque dans l'évaluation des risques pour la sécurité de la recherche. Le groupe de travail soumettra également des recommandations sur les outils et les mesures complémentaires qui garantiront que les chercheurs et les organismes de recherche — en collaboration avec les partenaires de la sécurité nationale — disposent de la capacité et des ressources nécessaires pour mettre en œuvre cette orientation. Le gouvernement du Canada a demandé que ces lignes directrices soient soumises aux fins d'examen d'ici le 25 juin 2021.

Lorsque ces lignes directrices deviendront disponibles, elles seront intégrées au processus d'évaluation de diligence raisonnable mené par le gouvernement du Canada à l'appui de cette initiative.

Comme les lignes directrices sont en cours d'élaboration, le gouvernement du Canada encourage les intervenants de l'écosystème canadien de recherche intéressés à participer au Réseau d'innovation pour la cybersécurité à collaborer dans le but d'identifier et d'atténuer les risques pour la sécurité en utilisant des outils existants disponibles dans le portail Protégez votre recherche et les ateliers de Science en sécurité.

Le gouvernement du Canada se réserve le droit de faire ce qui suit :

- examiner les projets du réseau à la lumière des enjeux de sécurité nationale pour s'assurer que les risques liés à la sécurité à l'échelle nationale sont identifiés et gérés;
- imposer aux bénéficiaires ultimes les obligations supplémentaires en matière de propriété intellectuelle nécessaires pour s'assurer que les risques pour la sécurité nationale soient atténués, au besoin;
- appliquer d'autres exigences, au cas par cas. Cela pourrait comprendre, sans toutefois s'y limiter, l'inspection de l'équipement (y compris l'infrastructure de TI) et des séances portant sur la sécurité, au besoin.

Le ministre se réserve le droit de refuser la participation de tout partenaire en invoquant n'importe quel motif pour préserver la sécurité et l'intégrité du réseau.

Partenaires de confiance

Seuls les partenaires de confiance qui respectent les plus hautes normes de sécurité et d'intégrité dans leurs activités, opérations et équipement, et qui ont de solides réputations et antécédents au Canada, seront admissibles pour participer au programme du Réseau d'innovation pour la cybersécurité.

Les principes qui définissent les partenaires de confiance du programme du Réseau d'innovation pour la cybersécurité comprennent les suivants :

- les principes dont les motifs et les intentions sont à la fois clairs et harmonisés aux buts du programme;
- les principes qui posent un faible risque pour la réputation en raison de la conformité antérieure démontrée aux normes internationales et aux valeurs de collaboration (p. ex., réciprocité, équité, honnêteté, etc.);
- les principes qui n'entraînent aucun conflit d'intérêts facilement discernable ou d'engagements conjoints qui nuiraient aux buts du programme;
- les principes qui respectent les normes éthiques et professionnelles les plus élevées, dont le respect des droits liés à la propriété intellectuelle, les données délicates et personnelles, les normes éthiques et les normes en matière de sécurité.

2.7 Langues officielles

Le bénéficiaire principal doit mettre à la disposition du public des communications et des services dans les deux langues officielles du Canada, conformément à l'esprit et à l'intention de la *Loi sur les langues officielles.*

Plus précisément, le bénéficiaire principal doit :

a. produire toute annonce ou tout document à l'intention des bénéficiaires ultimes dans la langue officielle de leur choix;
b. offrir activement ses services aux bénéficiaires ultimes dans la langue officielle de leur choix;
c. s'assurer que les communications destinées au grand public ou aux intervenants sont produites dans les deux langues officielles;
d. lorsque des services offerts par un bénéficiaire ultime font l'objet d'une demande importante par le public dans l'une ou l'autre des deux langues officielles, s'assurer que les ententes de financement conclues avec les bénéficiaires ultimes comprennent une clause exigeant que les communications des bénéficiaires ultimes à l'intention de la population respectent la demande linguistique.

ISDE respectera toutes les exigences applicables énoncées dans la *Loi sur les langues officielles du Canada*, sa réglementation connexe, ainsi que les politiques du gouvernement fédéral à ce sujet. Les communications publiques et les documents d'ISDE concernant le Réseau d'innovation pour la cybersécurité produits à des fins de diffusion publique seront disponibles dans les deux langues officielles.

2.8 Cadre de l'équité, de la diversité et de l'inclusion

Le bénéficiaire final devra mettre en œuvre un cadre de l'équité, de la diversité et de l'inclusion pour démontrer les mesures que prendra le réseau afin d'éliminer les obstacles à la participation des personnes de groupes sous-représentés au sein de la gouvernance, des opérations et des activités du Réseau, tels que définis dans la *Loi sur l'équité en matière d'emploi* du Canada (les femmes, les autochtones, les personnes handicapées et les personnes qui font partie des minorités visibles).

Les principes d'EDI sont définis comme suit dans le contexte du programme :

- L'**équité** se définie comme l'élimination des obstacles systémiques et des préjugés afin de permettre aux personnes d'avoir des chances égales d'accéder au programme et d'en bénéficier.
    - Pour y parvenir, les personnes qui participent à l'écosystème doivent développer une solide compréhension des obstacles systémiques et des préjugés auxquels se heurtent les personnes issues de groupes sous-représentés et mettre en place des mesures pour s'attaquer à ces obstacles.
- La **diversité** se définie par les différences sur les plans de la race, de la couleur, du lieu d'origine, de la religion, du statut d'immigrant et de nouvel arrivant, de l'origine ethnique, des capacités, du sexe, de l'orientation sexuelle, de l'identité de genre, de l'expression de genre et de l'âge.

  - Une diversité de perspectives et d'expériences personnelles est cruciale pour atteindre l'excellence dans le domaine de la recherche et de l'innovation.
- L'**inclusion** se définie comme étant la pratique de s'assurer que toutes les personnes soient appréciées et respectées pour leurs contributions et qu'elles soient appuyées de façon égale.
  - Pour atteindre l'excellence en matière de recherche et d'innovation, il est essentiel de veiller à ce que les membres soient intégrés et appuyés.

Le cadre de l'EDI doit au minimum respecter les exigences suivantes :

- inclure les objectifs, les mesures précises à mettre en œuvre pour atteindre les objectifs du cadre, les mesures de rendement, les résultats escomptés et les méthodes de collecte de données pour représenter les progrès pendant la période de financement;
- en ce qui concerne le conseil d'administration permanent et la haute direction, il faudra s'efforcer d'atteindre la cible de 50 p. 100 de parité entre les sexes et de 30 p. 100 de participation d'autres groupes sous-représentés (comme il est indiqué dans la section 2.2 Structure de gouvernance et gestion du présent guide);
  - Cette cible représente les objectifs aspirationnels du Défi 50-30, une initiative entre le gouvernement du Canada, les entreprises et les organisations en faveur de la diversité. Le but du programme est de lancer un défi aux organisations canadiennes pour qu'elles favorisent l'inclusion et augmentent la représentation des divers groupes dans leur milieu de travail, tout en faisant ressortir les avantages qu'il y a de donner à tous les Canadiens une place à la table des discussions. Le défi permet aux organismes participants de viser l'atteinte des objectifs du Défi 50-30 de la façon qui leur convient le mieux et en fonction de leurs besoins. On reconnaît ainsi la variété des tailles et des structures parmi l'ensemble des organismes, y compris ceux qui n'ont pas de conseil d'administration ou d'équipe de la haute direction.
- les critères de sélection pour des projets appuyés par le réseau et les membres des comités de sélection devront respecter les principes de l'EDI (indiqués à la section 2.3 Activités admissibles du présent guide).

2.9 Exigences relatives au financement de contrepartie

Le bénéficiaire principal devra fournir du financement de contrepartie équivalant à la contribution fédérale, selon un ratio de 1:1, totalisant 80 millions de dollars de plus sur quatre ans. Le financement devra être versé sous forme de contributions financières et/ou de contributions en nature. Le financement de contrepartie devra provenir de plusieurs partenaires autres que le gouvernement fédéral (p. ex., le secteur privé, les gouvernements provinciaux, territoriaux ou administrations municipales, et d'autres parties intéressées comme des organisations à but non lucratif et des établissements d'enseignement postsecondaire canadiens). La contribution équivalente à la contribution fédérale de 80 millions de dollars devrait permettre d'obtenir un investissement total minimal de 160 millions de dollars sur quatre ans.

Les demandeurs doivent démontrer comment ils comptent respecter les exigences du programme concernant le financement de contrepartie et inclure, au minimum, tous les besoins qui s'y rattachent pour les 12 premiers mois d'opérations au moment de soumettre la demande. Les contributions financières et/ou en nature de partenaires dans le cadre du financement de contrepartie seront exigées sous forme de lettres d'engagement à inclure dans la trousse de demande. La version finale

de toutes les conditions liées aux exigences concernant le financement de contrepartie figurera dans l'entente de contribution.

Contributions en nature

Les contributions en nature sont définies comme des biens ou des services équivalant à de l'argent comptant qui remplacent une dépense supplémentaire qui aurait dû être assumée au moyen de la contribution fédérale si elle n'avait pas été fournie par d'autres partenaires. Les contributions en nature doivent être fournies à leur juste valeur marchande et être pertinentes et reliées aux activités et aux objectifs de l'entente de contribution. Les contributions en nature pourraient comprendre de l'équipement (donné et/ou prêté), des coûts supplémentaires associés à l'accès aux bases de données, des matériaux, des logiciels, les salaires des chercheurs universitaires, etc. Les contributions en nature sont des coûts inadmissibles dans le cadre de la contribution fédérale du programme du Réseau d'innovation pour la cybersécurité.

Limites des contributions financières et en nature

Le tableau ci-dessous présente les limites des contributions financières et en nature permises dans le cadre du programme du Réseau d'innovation pour la cybersécurité.

	Année 1 (2021-2022)	**Année 2 (2022-2023)**	**Année 3 (2023-2024)**	**Année 4 (2024-2025)**
En nature	Jusqu'à 50 p.100	Jusqu'à 50 p. 100	Jusqu'à 25 p. 100	Jusqu'à 25 p. 100
Financières	Jusqu'à 50 p. 100	Jusqu'à 50 p. 100	Jusqu'à 75 p. 100	Jusqu'à 75 p. 100

Ventilation du financement

Contribution fédérale au Réseau d'innovation pour la cybersécurité (total de 80 millions de dollars sur quatre ans)	**Des contributions équivalentes provenant d'une combinaison de partenaires du secteur privé, d'établissements d'enseignement postsecondaire, de gouvernements provinciaux et territoriaux et d'administrations municipales et d'organisations à but non lucratif)** (total de 80 millions de dollars sur quatre ans)
• Le Réseau d'innovation pour la cybersécurité appuie les coûts admissibles financés. • Les coûts admissibles financés comprennent les coûts administratifs, opérationnels et liés aux projets. • Les contributions en nature sont des coûts inadmissibles.	• Les contributions équivalentes ont financé des coûts admissibles et/ou n'ont pas financé des coûts admissibles. • Le financement de coûts inadmissibles ne sera pas calculé dans le ratio 1:1 obligatoire du financement de contrepartie.

Financement supplémentaire

Les demandeurs sont encouragés à obtenir des contributions financières et/ou en nature excédant la contribution équivalente minimale obligatoire. Cependant, ces contributions supplémentaires ne peuvent être utilisées pour remplacer la contribution requise et le Réseau d'innovation pour la cybersécurité ne versera pas de contribution fédérale équivalente. Les contributions reçues d'autres sources, ou les contributions qui sont supérieures à la contribution fédérale maximale, peuvent être utilisées à la discrétion du bénéficiaire principal et des bénéficiaires ultimes, y compris pour les activités ou les coûts inadmissibles dans le cadre de ce programme. Les demandeurs sont tenus de divulguer tout soutien reçu d'autres programmes qui servira à appuyer le réseau et ses activités.

Le financement d'entités étrangères ne pourra faire partie des contributions financières ou en nature versées au réseau. Les locaux, les activités et l'équipement utilisés pour réaliser des activités financées par des gouvernements étrangers doivent être séparés de l'emplacement physique, de l'équipement et des activités du réseau.

2.10 Plan de viabilité du réseau

Le bénéficiaire principal devra élaborer un plan de viabilité qui décrit la stratégie visant à assurer une durabilité financière et à exploiter le réseau au-delà de la période de financement fédérale.

3. Processus de demande

Les demandeurs qui désirent présenter une demande auprès du Réseau d'innovation pour la cybersécurité doivent remplir la trousse de demande avant la date limite afin que leur demande fasse l'objet d'un examen. Le processus de demande et d'évaluation est anticipé comme suit :

3.1 Processus de présentation des demandes

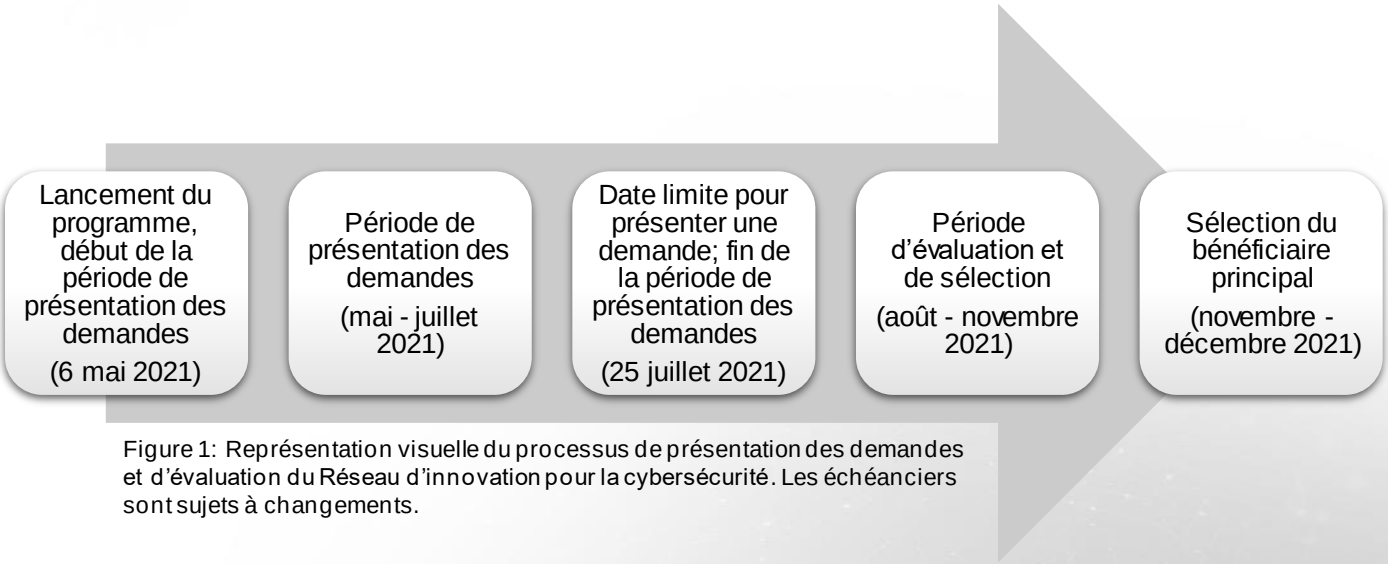

Figure 1: Représentation visuelle du processus de présentation des demandes et d'évaluation du Réseau d'innovation pour la cybersécurité. Les échéanciers sont sujets à changements.

Demandeur principal

Afin de présenter une demande au programme du Réseau d'innovation pour la cybersécurité, les réseaux demandeurs proposés doivent être représentés par un demandeur principal. Ce dernier sera responsable de présenter la demande et sera la personne-ressource pour ISDE pendant l'administration du processus de demande. Le demandeur principal peut être l'organisation à but non lucratif proposé pour gérer la contribution fédérale au chapitre du programme du Réseau d'innovation pour la cybersécurité, ou un participant qui assure un rôle principal dans le processus de demande au nom de ses partenaires. Les gouvernements fédéraux, provinciaux et territoriaux et les administrations municipales ne sont pas admissibles comme demandeur principal au même titre que les individus.

Les demandeurs sont invités à lire le guide du programme au moment de préparer leur trousse de demande.

Comment obtenir une trousse de demande

Pour obtenir la trousse de demande du Réseau d'innovation pour la cybersécurité, veuillez nous faire parvenir un courriel à l'adresse cybersecuritynetwork-reseaucybersecurite@ised-isde.gc.ca.

La trousse de demande contient les documents suivants :

- Formulaire de demande (Document Word)
- Annexe A : Historique financier des activités liées à la recherche et au développement, la commercialisation et le développement des compétences et talents en matière de cybersécurité (pour le demandeur principal et centres d'expertise en matière de cybersécurité affiliés à des établissements postsecondaires) (Document Excel)
- Annexe B – Liste des organismes qui participent au Réseau d'innovation pour la cybersécurité (Document Excel)
- Annexe C – Cahier de travail sur l'établissement des coûts et le financement (Document Excel)
    - Document de référence - Annexe D – Principes des coûts relatifs du programme de Réseau d'innovation pour la cybersécurité (Document PDF)

Les trousses de demande doivent être envoyées par courriel à l'adresse cybersecuritynetwork-reseaucybersecurite@ised-isde.gc.ca **au plus tard le dimanche 25 juillet 2021, à 23 h 59, heure normale du Pacifique (HNP).** Les demandes envoyées par la poste ou par télécopieur ne seront pas acceptées. Par souci d'équité pour tous les demandeurs, aucune prolongation ne sera accordée. Les demandeurs recevront un accusé de réception dans un délai de 48 heures ouvrables suivant la présentation de leur demande.

Les renseignements fournis dans la trousse de demande seront utilisés pour effectuer l'évaluation et le processus de sélection. Les demandes remplies ne seront pas examinées avant la fin de la période de présentation des demandes. Les demandes incomplètes ou qui, selon ISDE, ne respectent pas les critères d'admissibilité de base du programme ne seront pas évaluées et les demandeurs seront avisés par écrit.

4. Évaluation et processus de sélection

4.1 Processus d'évaluation

Le demandeur sélectionné sera choisi au moyen d'un processus transparent fondé sur le mérite pour déterminer si le demandeur est en mesure d'atteindre les objectifs et les résultats prévus du programme de contribution.

Les demandes de financement dans le cadre du Réseau d'innovation pour la cybersécurité seront évaluées en trois étapes, qui sont décrites ci-dessous.

4.1.1 Étape 1 – Présélection

Après la fin de la période de présentation des demandes, les responsables de programme du Réseau d'innovation pour la cybersécurité examineront les demandes pour :

- confirmer que les demandes soient complètes et exhaustives;
- confirmer l'admissibilité des demandeurs et les activités proposées.

Un avis écrit sera envoyé aux demandeurs pour les informer de l'évaluation ou du rejet, selon le cas, de leur proposition.

4.1.2 Étape 2 – Évaluation complète

ISDE formera un groupe consultatif en vue d'appuyer l'évaluation et le processus de sélection. Le groupe consultatif sera constitué d'experts en la matière provenant de l'ensemble du gouvernement du Canada, qui offriront une expertise et des connaissances pertinentes afin d'évaluer le mérite, le potentiel et la faisabilité d'une demande. Les demandes seront évaluées en fonction des quatre catégories de critères suivantes :

1. Activités proposées comparées aux trois piliers des activités du Réseau :

- recherche et développement;
- commercialisation;
- perfectionnement et développement des talents.

2. Exigences du programme décrites à la section 2 du guide du programme, notamment :

- la stratégie relative à la propriété intellectuelle;
- la stratégie relative à la gestion des données;
- le plan de cybersécurité;
- les exigences relatives au financement de contrepartie;
- le cadre de l'équité, de la diversité et de l'inclusion;
- la viabilité du réseau.

3. Avantages attendus pour le Canada

Avantages sur le plan de l'innovation

Les avantages sur le plan de l'innovation seront examinés en fonction des facteurs suivants :

- l'impact sur l'écosystème (p. ex., les participants du réseau sont représentatifs des régions du Canada; les participants du réseau représentent diverses organisations dans l'écosystème de la cybersécurité, notamment des PME, des grandes entreprises, des établissements d'enseignement postsecondaire; et le réseau complète les activités d'autres intervenants, dont des organisations à but non lucratif et des gouvernements provinciaux et territoriaux ou des administrations municipales);
- le niveau de collaboration (p. ex., y compris le financement de R-D et/ou des ressources en nature mis à contribution par le réseau pour des projets collaboratifs; des activités de réseautage proposées pour promouvoir la collaboration, etc.);
- le niveau d'innovation (p. ex., progression par rapport aux produits et services existants par opposition aux nouvelles approches et activités);
- les progrès technologiques (p. ex., la création et la commercialisation d'une nouvelle propriété intellectuelle au Canada);
- les retombées potentielles (p. ex., la création de capacités et de forces industrielles importantes et les avantages pour la chaîne d'approvisionnement élargie, l'industrie et/ou les partenaires, et une diversité d'intervenants).

Avantages économiques

L'évaluation des avantages économiques portera sur les facteurs suivants :

- la capacité de démontrer le degré de l'impact perturbateur potentiel du marché et l'avantage au sein du marché des technologies mises au point par le réseau (compétitivité);
- la voie à suivre menant à la commercialisation des projets appuyés par le réseau;
- le nombre d'emplois en cybersécurité créés en raison des activités et des initiatives du réseau.

Avantages pour le grand public

L'évaluation des avantages pour le grand public s'attardera aux facteurs suivants :

- la capacité de démontrer la croissance d'une réserve de personnes compétentes (p. ex., une évaluation des besoins de l'industrie en matière de compétences, un plan de formation ou de compétences en place dont des possibilités de formation, de requalification ou de perfectionnement, des occasions de stages coopératifs ou d'autres types d'apprentissage en milieu de travail, la diversification de la réserve de talents) qui peut répondre aux besoins ciblés de l'industrie et du milieu universitaire;
- la plus grande participation de groupes sous-représentés, en particulier les femmes, aux activités du réseau.

Autres avantages

- Les demandeurs sont encouragés à fournir des avantages supplémentaires pouvant découler de leur proposition et qui ne sont pas énumérés ci-dessus.

4. Évaluation de la diligence raisonnable

Le but est d'évaluer la capacité des demandeurs à atteindre les objectifs du programme. Les risques pris en compte comprennent les suivants :

- la gestion et la gouvernance;
- les moyens techniques et de la main-d'œuvre;
- la sécurité;
- la faisabilité financière;
- le risque commercial;
- impact sur le marché.

Non seulement le groupe consultatif doit évaluer les propositions en fonction des critères énumérés ci-dessus, le groupe consultatif pourrait également avoir à donner des conseils relatifs à des domaines possibles de collaboration en plus de tout ce qui figure dans une demande.

Tout au long du processus d'évaluation, ISDE pourrait inviter les demandeurs à prendre part à des réunions virtuelles avec le groupe consultatif afin de discuter plus à fond des propositions.

4.1.3 Étape 3 – Décision concernant le financement

Le groupe consultatif sera chargé d'examiner les résultats des évaluations et de fournir à ISDE une recommandation issue d'un consensus. Le ministre de l'Innovation, des Sciences et du Développement économique exercera son pouvoir discrétionnaire pour déterminer quelles propositions recevront du financement.

Les demandeurs retenus seront mis au courant de la décision finale à l'automne 2021 par l'entremise d'une lettre officielle du ministre d'ISDE.

Les décisions d'ISDE concernant le financement sont finales. Il n'y a pas de processus d'appel.

4.2 Entente de contribution

Après la sélection du projet, une entente de contribution entre le demandeur retenu et ISDE sera négociée, signée et exécutée et comprendra les responsabilités et les obligations exécutoires des deux parties. Certains éléments de la demande retenue pourraient être modifiés pendant les négociations de l'entente de contribution.

La valeur de l'entente de contribution conclue avec le bénéficiaire principal totalisera au plus 80 millions de dollars sur quatre ans (de 2021-2022 à 2024-2025). Le financement commencera à être versé selon la date négociée dans l'entente de contribution. Une entente de contribution décrira les

obligations de manière à accorder au réseau suffisamment de souplesse pour répondre aux dynamiques changeantes dans l'écosystème de l'innovation et au sein du marché tout au long de l'entente.

Le ministre de l'Innovation, des Sciences et de l'Industrie approuvera la première allocation de financement pour les activités admissibles en fonction de la demande du bénéficiaire principal et des plans organisationnels annuels subséquents, ce qui comprendra les besoins liés aux flux de trésorerie annuels (voir la section 5. Encadrement et surveillance pour obtenir de plus amples renseignements).

4.3 Dispositions relatives au cumul

Les demandeurs devront informer le ministre de toute autre aide financière gouvernementale (fédérale, provinciale, territoriale ou municipale) qu'ils ont reçue ou demandée. Le niveau combiné de l'aide financière de toutes les sources gouvernementales (fédérales, provinciales, territoriales et municipales) reçue par un demandeur admissible ne doit pas être supérieur à 75 p. 100 des coûts admissibles. Cette exigence ne s'applique pas aux demandeurs admissibles qui sont des établissements d'enseignement postsecondaire; ces derniers pourraient recevoir une aide totalisant 100 p. 100 des coûts admissibles.

Le niveau combiné de l'aide fournie au réseau par toutes les sources gouvernementales ne doit pas dépasser 100 p. 100 du total des coûts admissibles du réseau.

4.4 Méthode de paiement

Le bénéficiaire principal recevra des paiements en fonction des pièces justificatives pour les coûts admissibles réels engagés. Les demandes de remboursement doivent être soumises de manière individuelle par les bénéficiaires ultimes ou être combinées et présentées à ISDE par le bénéficiaire principal. Chaque demande de remboursement doit être accompagnée d'un bref rapport des travaux achevés et de renseignements détaillés au sujet des coûts visés par la demande de remboursement, en plus des pièces justificatives jugées satisfaisantes par le ministre. Les demandes de remboursement doivent être certifiées par un représentant du bénéficiaire principal ou par une personne exerçant des fonctions semblables et qui est jugée satisfaisante par le ministre.

Le réseau peut recevoir des paiements anticipés conformément à l'évaluation du niveau de risque et les besoins prévus pour le flux de trésorerie annuel du réseau fournis au ministre par le réseau. Pour chaque exercice financier, le réseau présentera des preuves satisfaisantes pour le ministre démontrant que tous les coûts admissibles ont été engagés et payés.

4.5 Conditions de remboursement

Les contributions versées dans le cadre du Réseau d'innovation pour la cybersécurité sont non remboursables.

5. Encadrement et surveillance

5.1 Plans organisationnels et rapports annuels

L'entente de contribution signée devra comprendre une disposition selon laquelle le bénéficiaire devra soumettre régulièrement des rapports d'étape, des rapports sur les demandes de remboursement et des états financiers annuels consolidés. Ces renseignements serviront à surveiller le rendement du réseau selon les dispositions de l'entente de contribution. Le bénéficiaire principal sera tenu de fournir des renseignements dans un plan organisationnel annuel et un rapport annuel.

5.1.1 Plan organisationnel

Le bénéficiaire principal doit présenter au ministre un plan organisationnel au plus tard le 31 janvier de chaque année d'exploitation. Le plan organisationnel doit comprendre les éléments suivants :

a. une référence au plan organisationnel du bénéficiaire principal pour l'exercice financier en cours (le cas échéant), y compris ses réussites et les défis qui persistent;
b. les objectifs et les activités prévus pour le prochain exercice financier, assortis d'un échéancier proposé pour leur mise en œuvre;
c. les dépenses prévues pour le prochain exercice financier;
d. l'évaluation des risques et les stratégies d'atténuation des risques;
e. les stratégies de surveillance continue du rendement;
f. les besoins annuels liés aux flux de trésorerie, y compris les plans pour satisfaire à l'exigence de financement de contrepartie selon le ratio 1:1 concernant les coûts admissibles pour le prochain exercice financier, notamment le financement à verser aux bénéficiaires ultimes pour des projets admissibles.

5.1.2 Rapport annuel

Le bénéficiaire principal doit présenter au ministre un rapport annuel dans les deux langues officielles du Canada au plus tard le 31 juillet de chaque année d'exploitation. Le rapport annuel doit comprendre les éléments suivants :

a. des renseignements sur les principaux indicateurs de rendement, les avantages des projets pour le Canada et les résultats obtenus au cours de l'exercice financier précédent;
b. les états financiers vérifiés pour l'exercice financier précédent, préparés selon les principes comptables généralement reconnus et approuvés par le conseil d'administration;
c. une déclaration concernant le financement total reçu par le bénéficiaire principal de toutes les sources au cours de l'exercice financier précédent, y compris l'aide gouvernementale canadienne, pour appuyer les activités admissibles;
d. une déclaration concernant le montant de la contribution affecté aux coûts admissibles au cours de l'exercice financier précédent, détaillé par catégorie d'activités admissibles;
e. le montant des contributions provenant d'autres sources (le cas échéant) reçu au cours de l'exercice financier précédent en appui aux activités admissibles;
f. un énoncé concernant les objectifs pour l'exercice financier précédent, comme ils sont indiqués dans le plan organisationnel pertinent, et une déclaration indiquant dans quelle

mesure le bénéficiaire principal a atteint ces objectifs ainsi que toute mesure corrective apportée ou tout écart par rapport aux objectifs initiaux;

g. un énoncé des objectifs pour l'exercice financier en cours et dans un avenir prévisible;
h. les critères utilisés pour choisir les activités admissibles des bénéficiaires ultimes.

Communications

Les activités et les résultats du bénéficiaire principal devraient être communiqués aux publics externes. Les communications doivent respecter les exigences en matière de langues officielles (voir la section 2.7 Langues Officielles pour obtenir de plus amples renseignements). Pour toute la durée de l'entente de contribution, les activités de communication et les messages du bénéficiaire principal doivent reconnaître la contribution du gouvernement fédéral à l'exécution de ces activités grâce au programme du Réseau d'innovation pour la cybersécurité, avec le mot-symbole Canada.

5.2 Surveillance, orientation et soutien

Les responsables de programme d'ISDE se chargeront de l'administration continue du programme. Ils travailleront avec le demandeur principal pendant les négociations relatives à l'entente de contribution, puis assureront un encadrement et une surveillance de manière continue une fois que l'entente de contribution aura été signée. ISDE assurera la liaison avec le bénéficiaire principal et pourrait notamment assister de temps à autre, à titre d'observateur, aux réunions du conseil d'administration et à d'autres réunions et/ou organiser des visites pour s'assurer que la mise en œuvre de l'entente de contribution est sur la bonne voie.

Des communications régulières et fréquentes faciliteront les échanges d'information entre les deux parties ayant conclu l'entente de contribution. L'administration par ISDE permettra de recueillir des renseignements afin d'orienter les politiques et les programmes fédéraux et de faciliter l'établissement de liens entre le bénéficiaire principal et d'autres organisations fédérales, s'il y a lieu.

5.3 Résultats attendus et indicateurs de rendement

Le bénéficiaire principal recueillera des renseignements qualitatifs et quantitatifs sur le rendement auprès des bénéficiaires ultimes afin de mesurer les progrès vers l'atteinte des résultats escomptés du réseau et sa capacité d'obtenir des résultats grâce aux activités proposées. Le tableau ci-dessous énumère les résultats attendus et les indicateurs de rendement qui doivent être fournis par le bénéficiaire principal. Les résultats attendus et les indicateurs de rendement peuvent être modifiés pendant les négociations de l'entente de contribution et les cibles seront négociées à ce moment-là en fonction de la proposition retenue.

Résultats à court terme (de 2021-2022 à 2022-2023)	
Résultats	**Indicateurs de rendement**
Impact de l'écosystème	
Portée nationale	Nombre de provinces/territoires représentés au sein du réseau
Inclusion complète de divers intervenants dans l'ensemble du pays	Nombre de participants du réseau provenant du milieu universitaire, du secteur privé, d'organisations à but non lucratif, entre autres, par type et emplacement géographique
Recherche et développement	
Collaboration de l'écosystème	Valeur financière et/ou en nature mise à contribution par le réseau et provenant du secteur privé et/ou d'autres partenaires
Perfectionnement et développement des talents	
Ressources (personnes et outils) accrues disponibles pour identifier, concevoir et offrir des solutions en matière de perfectionnement et de développement des talents	Le cadre du programme scolaire élaboré par le réseau se fonde sur une compréhension commune des besoins de l'industrie en matière de compétences
	Le nombre de nouveaux instructeurs ou formateurs en matière de cybersécurité, notamment des chefs de file de l'industrie et des praticiens recrutés dans des établissements d'enseignement postsecondaire grâce aux activités du réseau
Résultats à moyen terme (de 2023-2024 à 2024-2025)	
Résultats	**Indicateurs de rendement**
Recherche et développement	
Collaboration accrue entre l'industrie et le milieu universitaire	Nombre de projets collaboratifs de R-D auxquels participent l'industrie et le milieu universitaire
Commercialisation	
Les projets du réseau font progresser le développement de produits et de connaissances vers la commercialisation	Nombre de projets qui font progresser vers l'atteinte d'au moins deux niveaux de maturité technologique (NMT)
	Nombre de brevets déposés et/ou obtenus grâce aux activités du réseau
Perfectionnement et développement des talents	
Meilleures possibilités pour les étudiants et les travailleurs du domaine de la cybersécurité d'améliorer leurs compétences et d'approfondir leurs connaissances en matière de cybersécurité	Nombre de nouveaux étudiants d'établissements d'enseignement postsecondaire qui prennent part à des activités de formation en cybersécurité (cours, programmes, etc.)
	Nombre de participants issus de groupes sous-représentés, dont les femmes, qui participent à des activités de perfectionnement en matière de cybersécurité grâce au réseau

	Nombre de travailleurs dans les domaines liés à la cybersécurité qui participent à des formations connexes ou à des activités de requalification ou de perfectionnement offertes par le réseau
	Nombre d'étudiants d'établissements d'enseignement postsecondaire qui prennent part à des programmes coopératifs et/ou d'apprentissage en milieu de travail mis sur pied par le réseau
Résultats à long terme (de 2025-2026 à 2026-2027 et au-delà)	
Résultats	**Indicateurs de rendement**
Commercialisation	
Les entreprises canadiennes commercialisent des innovations nouvelles ou améliorées en matière de cybersécurité	Valeur des ventes de produits et services liés à la cybersécurité
Perfectionnement et développement des talents	
L'industrie peut accéder à une réserve de personnes qualifiées et compétentes en matière de cybersécurité	Nombre de personnes qualifiées dans le domaine de la cybersécurité
	Nombre de diplômés de programmes universitaires et de personnes formées qui intègrent la main-d'œuvre dans le domaine de la cybersécurité
	Pourcentage de professionnels issus de groupes sous-représentés, dont les femmes, qui se joignent à la main-d'œuvre dans le domaine de la cybersécurité.
	Pourcentage d'entreprises participant au réseau indiquant que les récents diplômés de programmes universitaires et personnes formées intégrant la main-d'œuvre dans le domaine de la cybersécurité répondent aux besoins de l'industrie

6. Politiques et considérations

6.1 *Loi sur l'accès à l'information* et *Loi sur la protection des renseignements personnels*

Le Réseau d'innovation pour la cybersécurité est assujetti à la *Loi sur l'accès à l'information* et à la *Loi sur la protection des renseignements personnels* du gouvernement fédéral.

6.2 Sécurité des renseignements

ISDE ne divulguera à aucune partie extérieure au gouvernement fédéral (autre que les parties externes choisies pour examiner les aspects techniques de la demande) les renseignements confidentiels de nature commerciale fournis par un demandeur, sauf dans les cas suivants :

- l'entreprise autorise la divulgation;
- la loi oblige ISDE à divulguer les renseignements;
- les renseignements cessent d'être confidentiels;
- le ministre d'ISDE est tenu de divulguer les renseignements à un groupe d'experts commerciaux international ou interne en raison d'un différend dans le cadre duquel le Canada est une partie ou un tiers intervenant.

S'il y a lieu, les demandeurs doivent indiquer dans leur proposition quels sont les renseignements confidentiels de nature commerciale. Il est également conseillé aux demandeurs de se familiariser avec les dispositions de la *Loi sur l'accès à l'information*, qui régit la divulgation de renseignements détenus par les organismes fédéraux.

Une copie électronique de toutes les demandes, peu importe l'issue du processus d'évaluation, sera conservée pendant dix (10) ans, après quoi elle sera détruite. Les demandes reçues à l'extérieur de la période visée pour la présentation des demandes seront retournées directement au demandeur sans avoir été lues ou évaluées.

6.3 *Loi sur le lobbying* et *Loi sur les conflits d'intérêts*

Dans le cadre du présent processus de demande, les demandeurs doivent fournir ce qui suit :

- une attestation selon laquelle tout individu, y compris tout consultant ou lobbyiste interne, qui fait du lobbying au nom du demandeur en vue d'obtenir du financement au titre du Réseau d'innovation pour la cybersécurité et qui doit être enregistré au titre de la *Loi sur le lobbying*, est effectivement enregistré conformément à cette loi. Pour obtenir de plus amples renseignements sur les activités de lobbying et la *Loi sur le lobbying*, veuillez consulter le Commissariat au lobbying du Canada;

- une attestation selon laquelle ni le demandeur ni qui que ce soit en son nom n'a embauché qui que ce soit (autre qu'un employé) dans le but d'obtenir du financement au chapitre du Réseau d'innovation pour la cybersécurité ou n'a versé ou convenu de verser à cette personne une

commission, des honoraires ou une rémunération en fonction des résultats ou toute autre contrepartie (pécuniaire ou autre) conditionnelle à l'obtention de financement au chapitre du programme;

- l'assurance que tout ancien fonctionnaire qui obtient des avantages de l'entente de contribution se conformera au *Code de valeurs et d'éthique du secteur public* à la *Politique sur la gestion des personnes* et à la *Directive sur les conflits d'intérêts;*

- l'assurance que tout ancien titulaire de charge publique qui tire un avantage de l'entente de contribution se conformera à la *Loi sur les conflits d'intérêts;*

- l'assurance qu'aucun membre de la Chambre des communes ou du Sénat ne tirera des avantages de l'entente de contribution;

- une attestation des principaux dirigeants confirmant que toute contribution versée dans le cadre du programme ne sera pas incluse dans l'évaluation de la rémunération au rendement des cadres supérieurs et ne servira pas à cette fin.

6.4 Accords internationaux

Le Réseau d'innovation pour la cybersécurité est géré conformément aux accords internationaux du Canada. Les contributions ne dépendent pas, en droit ou en fait, du rendement réel ou prévu en matière d'exportations.

7. Autre information

7.1 Site Web public

Le site Web d'ISDE fournit des renseignements sur les objectifs du programme, les exigences et la façon de présenter une demande dans le cadre du programme du Réseau d'innovation pour la cybersécurité.

7.2 Communiquez avec nous

Courriel
Pour joindre l'équipe du programme du Réseau d'innovation pour la cybersécurité, veuillez nous faire parvenir un courriel à l'adresse cybersecuritynetwork-reseaucybersecurite@ised-isde.gc.ca.

Téléphone
Centre de services aux citoyens d'ISDE
Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
ATS (pour les personnes malentendantes) : 1-866-694-8389
Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)

Adresse postale
Réseau d'innovation pour la cybersécurité
Édifice C.D. Howe
235, rue Queen, 9e étage, tour Est
Ottawa (Ontario) K1A 0H5
Canada

Définitions

Activités admissibles	Activités admissibles à du financement dans le cadre du programme du Réseau d'innovation pour la cybersécurité.
Avantages attendus	Avantages économiques, pour le grand public, sur le plan de l'innovation et autres qui devraient découler des activités du Réseau.
Centre d'expertise en matière de cybersécurité affilié à un établissement d'enseignement postsecondaire	Organisation affiliée à un établissement d'enseignement postsecondaire reconnu qui appuie la croissance de l'écosystème de l'innovation en matière de cybersécurité.
Conflit d'intérêts	Situation où, au détriment réel ou potentiel du Réseau d'innovation pour la cybersécurité, une personne participant au réseau est ou pourrait être en position de se servir du savoir de la recherche, de son autorité ou de son influence pour un gain personnel ou familial (financier ou autre) ou au profit d'autres personnes.
Contribution en nature	Les contributions en nature peuvent comprendre la juste valeur marchande d'une contribution autre que financière fournie au projet sous la forme de biens et/ou de services offerts par un partenaire. La juste valeur marchande s'entend du prix qui serait acceptable dans un marché ouvert et exempt de restrictions entre des parties informées et consentantes qui agissent de manière indépendante, qui sont bien renseignées et qui ne sont soumises à aucune pression.
Coûts admissibles	Coûts pour lesquels le programme du Réseau d'innovation pour la cybersécurité verse une contribution financière (pour couvrir le coût en tout ou en partie), comme il sera indiqué dans l'entente de contribution conclue avec le bénéficiaire principal.
Coûts inadmissibles	Coûts inadmissibles à un remboursement dans le cadre du programme du Réseau d'innovation pour la cybersécurité.
Cybersécurité	La protection de l'information numérique et de l'infrastructure sur laquelle elle repose.

Demande	Formulaire de demande dûment rempli et documents à l'appui soumis à ISDE aux fins d'examen dans le cadre du programme du Réseau d'innovation pour la cybersécurité.
Demandeur	Réseau formé d'au moins trois centres d'expertise canadiens en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire, des partenaires du secteur privé et autres, constitué comme une organisation à but non lucratif en vertu de la *Loi canadienne sur les organisations à but non lucratif*.
Demandeur principal	Le principal point de contact d'ISDE pendant le processus de présentation des demandes. Le demandeur principal peut être l'organisation à but non lucratif proposée pour gérer la contribution fédérale versée au chapitre du programme du Réseau d'innovation pour la cybersécurité, ou un participant qui forme le réseau et qui assume un rôle principal dans le processus de demande aux nom de ses partenaires. Les gouvernements fédéraux, provinciaux et territoriaux et les administrations municipales ne sont pas admissibles comme demandeur principal au même titre que les individus.
Diligence raisonnable	Méthode d'évaluation des demandes, qui examine la capacité des demandeurs de mettre en œuvre les activités et d'atteindre les objectifs énoncés dans la demande.
Entente de contribution	Entente écrite conclue entre le gouvernement du Canada et le demandeur retenu qui décrit les obligations et les accords des deux parties concernant le paiement de transfert. Après la signature de l'entente de contribution, le demandeur retenu est désigné comme le bénéficiaire principal. Le gouvernement du Canada est chargé de rédiger l'entente de contribution qui sera négociée avec le demandeur retenu.
Exercice financier	Conformément à la *Loi sur la gestion des finances publiques* (LGFP), un exercice financier s'entend de la période commençant le 1er avril d'une année et se terminant le 31 mars de l'année suivante.

Innovation, Sciences et Développement économique (ISDE)	Innovation, Sciences et Développement économique Canada est le ministère fédéral chargé d'administrer le programme du Réseau d'innovation pour la cybersécurité.
Lettre d'engagement	Démontre que le réseau a obtenu des contributions financières et/ou en nature des partenaires en vue de satisfaire à l'exigence relative au financement de contrepartie du programme du Réseau d'innovation pour la cybersécurité. Les lettres d'engagement doivent être signées par un cadre ayant le pouvoir d'autoriser la contribution (cadre de niveau C) et présentées sur du papier à en-tête officiel.
Organisations participantes (aussi désignées comme les participants du Réseau)	Les organisations participantes sont celles qui jouent un rôle dans la proposition du demandeur. Les types d'organisations participantes peuvent comprendre les suivants : ○ des centres d'expertise en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire (autres que les centres qui se présentent à titre de demandeurs); ○ des entités du secteur privé (y compris des petites et moyennes entreprises et des grandes entreprises); ○ des établissements d'enseignement postsecondaire canadiens (p. ex., centres de recherche, universités, collèges, polytechniques); ○ des organisations à but non lucratif (p. ex., associations industrielles, incubateurs et accélérateurs d'entreprises, organismes de perfectionnement de compétences, etc.); ○ des gouvernements provinciaux et territoriaux/administrations municipales. Les organisations participantes peuvent : • contribuer à l'exigence de fournir du financement de contrepartie et exécuter les activités liées à un projet; • exécuter des activités liées à un projet sans fournir un financement de contrepartie (p. ex., les bénéficiaires ultimes pourraient être choisis à l'issue d'un appel de propositions et recevoir uniquement du financement du réseau);

	• verser uniquement du financement de contrepartie (p. ex., consentir du financement au réseau et ne pas exécuter des activités liées à un projet); • se joindre au réseau sous une autre forme (à définir par le demandeur).
Partenaire	ISDE s'attend à ce que les catégories de partenaires suivantes, notamment, soient représentées dans la proposition de réseau : • centres d'expertise en matière de cybersécurité affiliés à des établissements d'enseignement postsecondaire (autres que les centres qui se présentent à titre de demandeurs); • secteur privé (y compris des petites et moyennes entreprises et des grandes entreprises); • établissements d'enseignement postsecondaire canadiens (p. ex., centres de recherche, universités, collèges, polytechniques); • organisations à but non lucratif (p. ex., associations industrielles, incubateurs et accélérateurs d'entreprises, organismes de perfectionnement de compétences, etc.); • gouvernements provinciaux et territoriaux/administrations municipales.
Projet	Les activités collectives réalisées pour atteindre les objectifs du programme du Réseau d'innovation pour la cybersécurité qui s'inscrivent sous trois piliers (recherche et développement; commercialisation; et perfectionnement et développement des talents).

Annexe A – Échelle des niveaux de maturité technologique

Niveau de maturité technologique	Description
NMT 1 – Observation et consignation des principes de base du concept	Niveau le plus bas de maturité technologique. La recherche scientifique commence à être convertie en recherche et développement. Les activités peuvent inclure les études sur les propriétés de base d'une technologie.
NMT 2 – Concept technologique ou application déterminé	Début des inventions. Une fois les principes de base observés, il s'agit de trouver les applications pratiques. Ces applications étant hypothétiques il se peut qu'elles ne n'appuient sur aucune preuve ni aucune analyse détaillée. Les activités sont limitées à des études analytiques.
NMT 3 – Fonction critique et analytique expérimentale ou validation de principe	La recherche et le développement active est lancée. Cette étape comprend des études analytiques et/ou en laboratoire. Les activités pourraient inclure des composants qui ne sont pas encore intégrés ou représentatifs.
NMT 4 – Validation des éléments ou des conditions d'essai en laboratoire	Les composants technologiques de base sont intégrés pour valider le bon fonctionnement commun. Les activités incluent l'intégration en laboratoire de matériel « spécial ».
NMT 5 – Validation des éléments ou des conditions d'essai en environnement simulé	Les composants technologiques de base sont intégrés, aux fins d'essais dans un environnement simulé. Les activités incluent l'intégration de composants en laboratoire.
NMT 6 – Démonstration d'un modèle ou d'un prototype du système ou du sous-système dans un environnement simulé	Le modèle ou le prototype représente une configuration quasi souhaitée. Les activités incluent l'essai dans un environnement opérationnel ou un laboratoire simulé. Les niveaux 7 à 9 représentent la phase de précommercialisation des innovations.
NMT 7 – Prototype prêt pour la démonstration dans un environnement opérationnel approprié	Le prototype a atteint l'état opérationnel prévu et est prêt pour la démonstration dans un environnement opérationnel. Les activités incluent l'essai du prototype sur le terrain.
NMT 8 – Technologie actuelle mise au point et qualifiée par des essais et des démonstrations	Il est prouvé que la technologie fonctionne dans sa forme finale et dans les conditions prévues. Les activités incluent des essais de mise au point et des évaluations afin d'établir si la technologie répond aux exigences opérationnelles.
NMT 9 – Validation de la technologie réelle par le déploiement réussi dans un contexte opérationnel	Application concrète de la technologie dans sa forme finale et dans des conditions réelles, comme celles s'appliquant au cours des essais et de l'évaluation opérationnels. Les activités incluent l'utilisation de l'innovation dans des conditions de conduite opérationnelle.