



National
Defence

Défense
nationale

CANADIAN
ARMED FORCES



FORCES ARMÉES
CANADIENNES

Bureau de recherche, d'ingénierie et de leadership avancés en matière d'innovation et de science (BOREALIS)

*De l'innovation à l'avantage opérationnel :
Carrefours sécurisés d'innovation pour la défense (CSID)*

GUIDE DU DEMANDEUR



Résumé des informations clés
• Mécanisme de financement : contribution non remboursable • Profil de financement annuel indicatif par CSID (non contraignant) : ○ Année 1 (exercice 2026-2027) : généralement entre 5 et 10 millions de dollars, selon la portée et l'ampleur des activités proposées pour la mise en place et la livraison initiale. ○ Année 2 (exercice 2027-2028) : généralement, entre 10 et 15 millions de dollars, selon la portée et l'ampleur des opérations à grande échelle et des activités programmatiques. • Durée de la contribution : jusqu'à la fin mars 2028 • Composition de l'équipe : les propositions doivent inclure des équipes multidisciplinaires composées de partenaires provenant d'au moins deux organisations et/ou institutions éligibles distinctes nécessaires à la réalisation des objectifs du CSID proposé • Une organisation canadienne admissible doit être désignée comme demandeur principal et agira en tant que bénéficiaire initial aux fins de l'accord de contribution.

1. Contexte

Les Carrefours sécurisés de l'innovation pour la défense (CSID) sont des carrefours sécurisés et axés sur des missions, créés pour permettre la collaboration entre le gouvernement, l'industrie et le milieu universitaire afin de soutenir les priorités du Canada en matière de défense et de sécurité nationale. Les CSID fournissent des environnements, des infrastructures et des services fiables qui soutiennent la conception, l'essai, la validation et la transition des technologies de pointe vers une utilisation opérationnelle.

Les CSID visent à combler une lacune persistante dans l'écosystème de l'innovation en matière de défense : bien que le Canada dispose d'une forte capacité de recherche et développement, les innovateurs se heurtent souvent à des obstacles pour s'engager auprès des organisations de défense, accéder à des environnements sécurisés et faire progresser les technologies au-delà des premières phases développement. Les CSID sont conçus pour soutenir à la fois les premiers stades d'engagement et les activités d'intégration plus avancées, notamment l'expérimentation, les essais et la transition dans des environnements sécurisés. Les CSID réduisent ces obstacles en permettant un engagement structuré, sécurisé et axé sur la mission avec les parties prenantes de la défense.

Chaque CSID se concentre sur un domaine de mission prioritaire défini et fonctionne comme un centre autonome doté d'une gouvernance et d'une responsabilité claires. Collectivement, les carrefours forment un réseau national qui soutient la mise en œuvre des capacités de défense et de sécurité. Les CSID sont mis en œuvre dans le cadre de BOREALIS, le mécanisme de coordination de l'innovation en matière de défense du gouvernement du Canada, qui assure la cohérence stratégique, l'harmonisation des programmes fédéraux d'innovation et un guichet unique pour la participation aux initiatives prioritaires d'innovation en matière de défense et de sécurité.

2. Le défi

Les organisations canadiennes de défense et de sécurité nationale opèrent dans un environnement caractérisé par des changements technologiques rapides, une complexité croissante des systèmes et des exigences de sécurité accrues. Deux domaines technologiques en particulier, **les technologies quantiques** et **les systèmes sans pilote (UxS)**, devraient avoir un impact significatif sur les futures opérations de défense et de sécurité. Si l'innovation dans ces deux domaines progresse rapidement dans les milieux universitaires et industriels, des défis subsistent pour faire progresser ces technologies vers des applications de défense et de sécurité. **Des informations supplémentaires sur les domaines de défi liés aux technologies quantiques et aux UxS sont fournies à l'annexe A.**

Quantique

Dans le domaine quantique, le Canada dispose de solides capacités de recherche et d'innovation dans les domaines de la détection, des communications, de l'informatique et de la cryptographie. Cependant, le passage des technologies quantiques des démonstrations en laboratoire aux applications de défense et de sécurité présente des défis particuliers. Il s'agit notamment de la nécessité d'avoir accès à **des infrastructures spécialisées, à des environnements sécurisés et à des cas d'utilisation pertinents pour la défense** permettant de tester et de valider les technologies. Les innovateurs n'ont souvent pas les moyens de collaborer suffisamment tôt avec les acteurs de la défense pour garantir la pertinence opérationnelle, tandis que les organismes de défense ont du mal à évaluer la maturité, les risques et le potentiel d'intégration dans un domaine en rapide évolution et hautement spécialisé.

À mesure que les technologies quantiques approchent du seuil de pertinence opérationnelle, il devient de plus en plus nécessaire de disposer d'environnements qui permettent **des expérimentations sécurisées, l'intégration au niveau des systèmes et la validation** dans des conditions qui reflètent les contraintes de la défense et de la sécurité nationale. Sans de tels environnements, les technologies prometteuses risquent de rester déconnectées des besoins réels de la défense ou d'évoluer dans des directions qui ne correspondent pas aux priorités opérationnelles.

Systèmes autonomes et sans pilote (UxS)

Dans le domaine des UxS, l'innovation couvre les plateformes, les capteurs, les communications, les logiciels d'autonomie et les systèmes habilitants. Si de nombreuses technologies UxS se révèlent prometteuses à leurs débuts, leur mise en œuvre dans des contextes de défense et de sécurité nécessite de surmonter des défis liés à la sécurité des essais, à l'intégration avec les systèmes existants, à l'interopérabilité, à la conformité réglementaire et à la validation par rapport aux concepts opérationnels.

Les innovateurs sont souvent confrontés à un accès limité aux utilisateurs de la défense, à des environnements de test contrôlés et à des possibilités d'intégrer leurs technologies dans des systèmes de systèmes plus larges. Parallèlement, les organisations de défense doivent évaluer non seulement les composants individuels, mais aussi les performances des systèmes sans équipage et autonomes lorsqu'ils sont intégrés, exploités à grande échelle et déployés dans des environnements contestés ou contraints.

Les environnements sécurisés, un défi transversal

Dans les domaines quantique et UxS, l'un des principaux obstacles est le **manque d'accès à des environnements de collaboration sécurisés**. De nombreuses activités nécessaires pour faire progresser les technologies vers une pertinence opérationnelle, telles que l'intégration, les tests au niveau du système et la validation avec les utilisateurs de la défense, ne peuvent être menées dans des environnements ouverts ou non classifiés.

Les organisations de défense et de sécurité nationale ont besoin d'environnements pouvant prendre en charge des travaux à **des niveaux de sécurité élevés**, notamment des installations et des environnements numériques pouvant être **accrédités jusqu'au niveau II (secret)**. La mise en place et l'exploitation de tels environnements sont complexes et nécessitent des ressources importantes, ce qui dépasse souvent les capacités des innovateurs ou des organisations agissant seuls. L'absence d'environnements sécurisés

partagés et fiables représente donc un défi systémique pour la transition des technologies émergentes vers des applications de défense et de sécurité.

Objectif de la mission

Aux fins du présent appel de propositions, l'**expression « axé sur la mission »** désigne les activités qui s'inscrivent dans des cas d'utilisation liés à la défense et à la sécurité nationale, qui tiennent compte des contraintes opérationnelles et qui sont adaptées aux besoins des utilisateurs finaux visés. L'orientation vers la mission va au-delà du développement technologique et tient compte de la manière dont les capacités sont intégrées, testées, validées et transférées dans des contextes réels de défense et de sécurité. Dans le domaine **quantique**, les activités axées sur la mission peuvent inclure le développement de technologies vers des applications pertinentes pour la défense, telles que la détection, la mise en réseau ou l'informatique dans le respect des contraintes de sécurité, d'intégration et d'exploitation. Dans le domaine **UxS**, les activités axées sur la mission peuvent inclure le développement de systèmes autonomes et sans équipage et de technologies habilitantes grâce à l'intégration, aux essais et à la validation au niveau du système, en accord avec les concepts d'opération de défense.

Relever le défi grâce au CSID

Cet appel à propositions vise à relever ces défis en créant **des Carrefours sécurisés de l'innovation pour la défense (CSID)** axés sur les domaines de mission **quantique** et **UxS**. Les CSID ont pour objectif de fournir **des environnements sécurisés et axés sur les missions** où le gouvernement, l'industrie et le monde universitaire peuvent collaborer au fil du temps pour faire progresser les technologies au-delà du stade du développement initial et vers des applications de défense et de sécurité.

Grâce à l'accès à des environnements et à des infrastructures fiables et à un engagement soutenu avec les acteurs de la défense, les CSID permettront de mener des activités telles que l'expérimentation, les essais, l'intégration des systèmes et la validation, favorisant ainsi des transitions plus claires entre l'innovation et l'acceptation opérationnelle.

3. Admissibilité

Cet appel de propositions est ouvert aux propositions soumises par des organisations canadiennes éligibles, en partenariat avec d'autres organisations éligibles, en vue de créer et d'exploiter un CSID.

Les organisations ou institutions **demandeurs principales** admissibles sont les suivantes :

- Les organisations canadiennes à but lucratif constituées en société ;
- Les organisations canadiennes à but non lucratif constituées ;
- Les universités canadiennes ou autres établissements d'enseignement postsecondaire agréés au Canada.

Le demandeur principal agira à titre de bénéficiaire aux fins de l'accord de contribution et assumera la responsabilité globale du CSID proposé.

Les **organisations** ou établissements **partenaires** admissibles sont les suivants :

- Les universités canadiennes et autres établissements d'enseignement postsecondaire agréés au Canada ;

- Les organisations canadiennes à but lucratif constituées ;
- Les organisations canadiennes à but non lucratif constituées ;
- Les organisations gouvernementales provinciales, territoriales et municipales canadiennes.

Toutes les organisations/institutions doivent posséder le statut juridique nécessaire pour conclure un accord de contribution.

Les ministères, organismes et sociétés d'État fédéraux ne sont pas admissibles au financement. De plus, les propositions ne doivent pas supposer ou inclure l'utilisation d'infrastructures ou d'installations appartenant au gouvernement fédéral, y compris celles détenues ou exploitées par le ministère de la Défense nationale ou les Forces armées canadiennes, dans le cadre du CSID proposé.

3.1 Composition de l'équipe CSID

Chaque proposition doit désigner un **demandeur principal (bénéficiaire initial)** et une ou plusieurs **organisations partenaires (bénéficiaires finaux)** qui, ensemble, forment l'équipe de mise en œuvre du CSID.

Le **demandeur principal** est responsable de la gouvernance, du fonctionnement et de la gestion globaux du CSID et servira de point de contact principal avec le ministère de la Défense nationale (MDN) tout au long du processus de demande et de la période de financement. Le demandeur principal doit accepter d'assumer la responsabilité administrative et financière du CSID.

Le demandeur principal doit remplir les rôles et responsabilités suivants :

- Agir en tant que signataire de l'accord de contribution avec le MDN au nom du CSID.
- S'assurer que tous les coûts soumis au MDN sont admissibles.
- Recevoir, gérer et distribuer les fonds de contribution, le cas échéant, aux organisations partenaires à l'appui des activités admissibles.
- Établir et gérer les accords avec les organisations partenaires, y compris les arrangements relatifs à la collaboration, aux flux de financement et à la propriété intellectuelle, selon les besoins.
- Surveiller les activités et les résultats obtenus conformément aux exigences de l'accord de contribution et en rendre compte au MDN.

Les organisations partenaires contribuent à la mise en œuvre du CSID en fournissant l'expertise, l'infrastructure, les services ou les capacités nécessaires pour atteindre les objectifs du carrefour proposé. Les organisations partenaires peuvent recevoir un financement dans le cadre du présent appel à propositions par l'intermédiaire du demandeur principal et doivent conclure des accords appropriés avec celui-ci pour remplir leurs fonctions.

Les propositions doivent inclure des équipes multidisciplinaires composées de partenaires provenant d'au moins deux organisations et/ou institutions éligibles distinctes.

3.2 Activités CSID admissibles

Les demandes doivent inclure à la fois :

- Une **infrastructure sécurisée** : une approche crédible et bien justifiée pour l'aménagement des installations existantes, la maintenance et l'exploitation d'une infrastructure CSID sécurisée, y compris un plan par étapes pour obtenir l'accréditation aux niveaux de sécurité appropriés au cours de la période de financement, et

- **Plan de R&D** : un programme de recherche et développement (R&D) substantiel et cohérent à mettre en œuvre grâce à cette infrastructure, aligné sur un ou plusieurs des domaines de défi identifiés dans le présent appel à propositions (Quantique et systèmes sans pilote (UxS)).

Les activités admissibles peuvent inclure, sans s'y limiter :

- Mise en place, aménagement, maintenance et exploitation d'environnements physiques et/ou numériques sécurisés, y compris les modifications à apporter à l'infrastructure existante nécessaires pour permettre un travail collaboratif sécurisé au niveau II (Secret), dans le cadre d'une capacité de carrefour plus large. Ces activités ne peuvent dépasser 50 % du coût total proposé. Voir l'annexe C pour plus de détails. Remarque : les installations ne sont pas tenues d'être accréditées au niveau II (Secret) au moment de la demande ; les propositions doivent plutôt démontrer un plan crédible pour atteindre le niveau de sécurité approprié pendant la période de financement.
- Conception et mise en œuvre d'activités de R&D programmatiques permettant l'expérimentation, les tests, l'intégration des systèmes et la validation.
- Fourniture de services techniques, opérationnels et de coordination qui soutiennent la collaboration entre le gouvernement, l'industrie et le monde universitaire.
- Activités d'engagement et de facilitation qui mettent en relation les innovateurs avec les acteurs de la défense et de la sécurité.
- Activités qui soutiennent la transition et l'adoption de technologies en vue de leur application dans le domaine de la défense et de la sécurité nationale

Les activités liées à de nouvelles constructions ne sont pas admissibles dans le cadre du présent appel de propositions.

4. Financement

4.1 Financement disponible et durée

Le financement dans le cadre du présent appel à propositions est fourni par BOREALIS et versé par l'intermédiaire du **programme Innovation pour la défense, l'excellence et la sécurité (IDEeS)** afin de soutenir la **création et le fonctionnement à durée limitée des CSID**.

Le financement sera accordé sous la forme d'une **contribution non remboursable** dans le cadre d'un accord de contribution entre le gouvernement du Canada et le demandeur principal retenu.

Durée de la contribution

Les accords de contribution résultant du présent appel de propositions peuvent avoir une durée **maximale de 24 mois**, les activités devant s'achever **au plus tard par la fin du mois de mars 2028**.

Enveloppe financière totale

À des fins de planification, le gouvernement du Canada prévoit une **enveloppe de financement totale pouvant atteindre 50 millions de dollars** dans le cadre de cet appel de propositions, sous réserve de la réception de propositions de qualité suffisante.

Profil indicatif du financement annuel

À des fins de planification uniquement, les demandeurs doivent prendre note des **prévisions de financement annuel indicatives** suivantes, sur la durée maximale de l'accord de contribution. **Les besoins de financement peuvent varier en fonction du domaine, de la portée et de la nature du CSID proposé.**

Année 1 (exercice 2026-2027) :

Le financement soutient les activités de mise en place, notamment le développement d'un environnement sécurisé, les opérations initiales et la mise en œuvre rapide des activités du centre. Un financement d'environ 5 à 10 millions de dollars pourrait être approprié, selon la portée et l'ampleur des activités proposées. Les demandeurs doivent demander un financement raisonnable et bien justifié.

Année 2 (exercice 2027-2028) :

Le financement soutient les opérations à grande échelle et l'augmentation des activités programmatiques après la mise en place du CSID. Un financement d'environ 10 à 15 millions de dollars pourrait être approprié, en fonction de la portée et de l'ampleur des activités proposées.

Ces chiffres sont **indicatifs et non contraignants** et ne représentent pas des plafonds ou des garanties de financement.

Flexibilité du financement

Le gouvernement du Canada se réserve le droit :

- Financer les propositions à des niveaux **inférieurs aux montants demandés**
- **Ajuster les profils de financement** au cours des exercices financiers
- **Négocier la portée, les étapes et les niveaux de financement** avant de finaliser les accords de contribution

4.2 Dispositions cumulatives et autres aides gouvernementales

L'aide totale accordée par le gouvernement canadien (fédéral, provincial/territorial et municipal) ne peut dépasser 100 % du coût total de la proposition. Les demandeurs doivent indiquer toutes les sources de financement dans leur proposition et confirmer ces informations dans un accord de contribution si la proposition est sélectionnée pour bénéficier d'un financement.

4.3 Coûts admissibles

Les coûts admissibles sont ceux qui sont approuvés et engagés par le demandeur principal et les organisations partenaires et qui, de l'avis du MDN, sont raisonnables et nécessaires à la réalisation des activités admissibles du CSID. Les coûts admissibles se limiteront aux coûts réels, non récurrents et supplémentaires du demandeur principal et des organisations partenaires qui sont directement liés à la mise en place et au fonctionnement du CSID approuvé et qui sont nécessaires pour atteindre les résultats escomptés. De plus amples détails sur les coûts admissibles et non admissibles sont fournis à l'annexe C – Coûts admissibles et non admissibles.

4.4 Contenu canadien

En règle générale, les coûts admissibles, dans toutes les catégories de coûts, doivent être engagés au Canada. Toutefois, IDEES peut soutenir des activités admissibles et des coûts connexes engagés à l'extérieur du Canada lorsque ces dépenses sont nécessaires pour atteindre les objectifs de la proposition. Dans tous les cas, pas plus de 50 % des coûts admissibles peuvent être engagés à l'extérieur du Canada. Les CSID doivent veiller au respect de cette exigence.

4.5 Autres sources de financement : contributions en espèces et en nature

Les demandeurs sont encouragés, mais non tenus, à démontrer la pertinence, la durabilité et la collaboration en tirant parti des contributions en espèces et/ou en nature provenant d'autres sources à l'appui du carrefour sécurisé de l'innovation pour la défense (CSID) proposé.

Les contributions en nature sont des biens ou des services équivalents à des espèces fournis par une organisation au CSID qui représentent une dépense supplémentaire qui devrait autrement être engagée pour mener à bien les activités proposées du carrefour. Il peut s'agir, par exemple, de l'accès à des installations ou à des infrastructures, à des données, à des logiciels, à la propriété intellectuelle, au temps de travail du personnel ou à des équipements spécialisés.

Les contributions en espèces peuvent être utilisées pour compléter le financement IDEEs en soutenant des activités supplémentaires, en renforçant les capacités du carrefour ou en élargissant la portée des opérations CSID au-delà de ce qui pourrait être réalisé grâce au seul financement IDEEs.

Le cas échéant, les contributions en espèces et en nature doivent être clairement décrites dans la proposition, y compris leur source, leur nature et leur utilisation prévue. Les contributions fournies par les organisations partenaires ou des tiers doivent être gérées par le demandeur principal conformément aux accords appropriés conclus entre les organisations participantes.

5. Formulaire de proposition et soumission

5.1 Formulaire de proposition

Les demandeurs doivent utiliser le formulaire de proposition des *Carrefours sécurisés de l'innovation pour la défense (CSID)*. Les demandeurs sont et resteront seuls responsables de l'exactitude et de l'exhaustivité de leur soumission. Les demandeurs doivent lire le Guide du demandeur et l'énoncé du défi dans son intégralité avant de soumettre leur proposition.

La proposition doit être soumise par un demandeur principal admissible (voir 3.1) avant la date limite indiquée. Aucune proposition ne sera acceptée après la date limite. Les propositions qui n'utilisent pas le formulaire de proposition CSID ne seront pas prises en considération.

Les demandeurs peuvent soumettre plusieurs propositions, mais chacune d'entre elles doit être distincte, autonome et indépendante des autres. Si les propositions sont jugées dépendantes les unes des autres, elles seront considérées comme irrecevables et ne seront pas prises en considération.

Les personnes appartenant à des organisations admissibles peuvent également participer à plusieurs CSID. Dans ce cas, toutes les activités de R-D doivent être propres à chaque CSID et ne doivent pas dépendre ou chevaucher les activités d'un autre CSID. Les bénéficiaires participant à plusieurs propositions sélectionnées doivent soumettre des rapports financiers distincts pour chaque CSID. Seuls les coûts admissibles directement liés à la réalisation des objectifs du CSID spécifique financé par le MDN peuvent être inclus.

Date limite de soumission : 14 h (heure de l'Est), le jeudi 2 avril 2026.
--

Dans leur proposition, les demandeurs doivent démontrer leur capacité et décrire leur approche de manière exhaustive, concise et claire pour mener à bien les travaux. Les réponses du demandeur dans le formulaire de proposition seront utilisées pour élaborer l'annexe A de l'accord de contribution pour le CSID. La proposition doit aborder de manière claire et suffisamment approfondie les points qui font l'objet des critères d'évaluation sur la base desquels la proposition sera évaluée.

Afin de préserver l'intégrité de l'évaluation, les évaluateurs ne tiendront compte que des informations présentées dans la proposition. Aucune information ne sera déduite et les connaissances ou convictions

personnelles ne seront pas utilisées dans l'évaluation. Les demandeurs doivent démontrer de manière explicite et suffisamment détaillée comment tous les critères sont remplis.

Les lettres d'appui, de recommandation ou de soutien ne seront pas acceptées ni prises en compte dans le cadre de la proposition. Les demandeurs ne doivent pas soumettre de lettres d'appui ni y faire référence dans leurs réponses. Tout document de ce type, s'il est soumis ou mentionné, ne sera pas pris en compte dans le processus d'évaluation.

Tous les coûts indiqués dans la proposition doivent être exprimés en dollars canadiens.

Il incombe au demandeur de s'assurer que la demande et toutes les activités proposées sont conformes à toutes les lois fédérales, provinciales et territoriales pertinentes ainsi qu'aux règlements municipaux.

5.2 Soumission de la proposition

Les demandeurs doivent s'inscrire et soumettre leur(s) proposition(s) à l'aide du [Le service Connexion](#) fourni par la Société canadienne des postes (CPC). Connexion est une plateforme de livraison numérique qui facilite l'envoi et la réception de messages et de documents confidentiels. Les propositions soumises par courrier électronique ne seront pas acceptées. Il incombe au demandeur de créer un compte sur CPC Connexion et de suivre toutes les étapes requises pour soumettre la proposition. Les demandeurs doivent demander leur conversation le service Connexion au moins cinq (5) jours avant la date de clôture de l'appel à propositions.

Les propositions classifiées ne seront pas acceptées pour cet appel à propositions.

Processus de soumission

#	Action	Détails
1.	Créer un compte CPC Connexion	Compte existant : - Si vous possédez déjà un compte, passez à l'étape 2. Inscription d'un nouveau compte : - Créez un compte sur CPC Connexion. - Cliquez sur « Se connecter à Connexion » sur la page Web CPC Connexion. - Sélectionnez « S'inscrire maintenant » et remplissez votre profil personnel Canada Post. - Remarque : L'inscription est gratuite.
2.	Demander une conversation Connexion	Comment faire une demande : - Envoyez un courriel à borealisjointprogramoffice-bureaudeprogrammeintegreborealis@forces.gc.ca pour demander une conversation Connexion. - Le courriel doit être envoyé au moins cinq (5) jours ouvrables avant la date de clôture de l'appel de propositions. - Une fois la demande effectuée, l'équipe BOREALIS lancera la conversation Connexion. Notification par courriel : - Le demandeur recevra une notification par courriel de la part du CPC l'invitant à accéder à la conversation.

		- Grâce à cette conversation, le demandeur pourra soumettre sa proposition avant la date limite de l'appel à propositions. Important : - Chaque proposition doit avoir un titre et un numéro de dossier uniques (attribués par l'équipe BOREALIS). - Lorsque vous demandez une conversation, indiquez le nombre de propositions afin de vous assurer que des numéros de dossier individuels sont attribués.
3.	Soumettez la proposition via CPC Connexion	Téléchargez votre proposition : - Soumettez la proposition en la téléchargeant dans la conversation Connexion - Assurez-vous que la soumission ait lieu avant la date et l'heure de clôture de l'appel de propositions. Confirmation : - Un message de confirmation sera affiché dans la conversation Connexion après la soumission ou après la clôture de l'appel à propositions. - Assurez-vous que la proposition comprend les coordonnées complètes du demandeur.

5.3 Problèmes de transmission ou soumissions tardives

Le MDN ne sera pas responsable des défaillances attribuables à la transmission ou à la réception de la proposition, y compris, mais sans s'y limiter, les suivantes :

- Réception d'une proposition illisible, corrompue, incomplète ou illisible ;
- Incompatibilité des équipements ou des systèmes ;
- Perturbations ou erreurs du service CPC Connexion
- Retards de toute nature ;
- Impossibilité d'établir une conversation électronique ; ou
- Sécurité des données de la proposition.

Les soumissions tardives ne seront pas acceptées.

6. Évaluation des propositions

Les propositions seront examinées selon les critères énumérés à l'annexe B, Critères d'évaluation.

Les propositions seront examinées par des experts en la matière sélectionnés par BOREALIS et pouvant inclure des représentants d'autres ministères du gouvernement canadien.

BOREALIS peut sélectionner une proposition, plusieurs propositions ou aucune proposition à des fins de financement. À ce stade, tous les demandeurs seront informés du statut de leur proposition après évaluation.

Les demandeurs dont les propositions auront été sélectionnées pourraient être invités à fournir des renseignements supplémentaires à l'appui des décisions finales de sélection pour le financement. Une analyse supplémentaire des propositions pourrait être nécessaire, notamment des évaluations des risques

financiers et des évaluations techniques. Le défaut de fournir en temps opportun les renseignements à l'appui de ces analyses pourrait entraîner l'élimination du processus.

Avant de prendre une décision finale, le MDN peut solliciter l'avis et les conseils d'autres organisations, notamment des organismes et organisations gouvernementaux fédéraux, provinciaux, territoriaux et municipaux.

7. Déclaration de confidentialité

Le MDN se conformera à la [Loi sur l'accès à l'information](#) et à la [Loi sur la protection des renseignements personnels](#) du gouvernement fédéral en ce qui concerne les propositions reçues. En soumettant des renseignements personnels, le demandeur consent à leur collecte, à leur utilisation et à leur divulgation conformément à l'avis de confidentialité suivant, qui explique comment les renseignements du demandeur seront gérés.

Les mesures nécessaires ont été prises pour protéger la confidentialité des renseignements fournis par les demandeurs. Ces renseignements sont recueillis en vertu des modalités du programme de paiements de transfert IDEeS du MDN.

Les renseignements personnels contenus dans toutes les propositions seront conservés avec les résultats des propositions à titre de documents d'information ayant une valeur opérationnelle. Ces renseignements sont protégés en vertu de la *Loi sur l'accès à l'information et la protection des renseignements personnels*. Conformément à la *Loi sur la protection des renseignements personnels*, les données liées à une personne et contenues dans la proposition évaluée peuvent être consultées par la personne concernée qui détient des droits à l'égard de ces renseignements. Cette personne peut, sur demande :

- (1) obtenir l'accès à ses données en présentant une demande officielle de confidentialité au MDN à l'attention du directeur, Accès à l'information et protection des renseignements personnels (DAIPRP), et
- (2) faire corriger les informations incorrectes ou y joindre une note.

La *Loi sur l'accès à l'information* régit la protection et la divulgation des renseignements, confidentiels ou non, fournis à une institution fédérale.

L'alinéa 20(1)b) de la Loi stipule que :

Une institution fédérale [telle que le MDN] refuse de communiquer tout document demandé en vertu de la Loi qui contient des renseignements financiers, commerciaux, scientifiques ou techniques qui sont des renseignements confidentiels fournis à une institution fédérale par un tiers et qui sont traités de manière confidentielle par ce tiers.

L'alinéa 20(1)b) de la Loi énonce deux critères obligatoires afin de protéger les renseignements confidentiels fournis au MDN par les demandeurs contre la divulgation. Premièrement, les documents fournis au MDN par les demandeurs doivent contenir des renseignements financiers, commerciaux, scientifiques ou techniques. Deuxièmement, le demandeur doit traiter ces renseignements de manière confidentielle. En d'autres termes, le MDN protégera les renseignements confidentiels du demandeur en sa possession autant que le demandeur protège ces renseignements confidentiels dans son propre établissement.

Toute demande relative à la protection des renseignements personnels ou à l'accès à l'information présentée en vertu de la loi applicable et traitée sera conservée par le DAIPRP pendant une période de deux (2) ans à compter de la date à laquelle la demande a reçu une réponse. Après la période de

conservation de deux (2) ans, le dossier de la demande relative à la protection des renseignements personnels ou à l'accès à l'information sera détruit.

Pour obtenir des renseignements supplémentaires sur les questions de confidentialité avant de soumettre une proposition, veuillez communiquer avec :

Directeur, Accès à l'information et protection des renseignements personnels (DAIPRP)

Ministère de la Défense nationale (MDN)

Téléphone : ligne directe : 613-992-0996 ou sans frais : 1-888-272-8207

Courriel : ATIP-AIPRP@forces.gc.ca

Les demandeurs doivent noter que les informations clés relatives à tous les accords de contribution (par exemple, le montant, le nom des bénéficiaires initiaux et finaux et leur emplacement) seront rendues publiques sur le site web du MDN.

8. Demandes de renseignements sur l'appel de propositions

Il incombe au demandeur d'obtenir des précisions sur les informations contenues dans le présent document avant de soumettre sa candidature.

Les demandes de renseignements relatives au présent appel de propositions doivent être envoyées à BOREALIS à l'adresse borealisjointprogramoffice-bureaudeprogrammeintegreborealis@forces.gc.ca, avec pour objet « Question CSID appel de propositions », au plus tard cinq (5) jours civils avant la date de clôture de l'appel de propositions. Les demandes de renseignements reçues après cette date limite pourraient ne pas recevoir de réponse. Les demandeurs doivent clairement mentionner le numéro de la section pertinente du présent appel de propositions et fournir suffisamment de détails pour permettre une réponse précise.

Les questions et réponses reçues pendant la période de l'appel à propositions peuvent être mises à la disposition de tous les demandeurs.

9. Accord de contribution

Les demandeurs dont les propositions auront été retenues seront invités à conclure un accord de contribution avec le MDN.

BOREALIS travaillera avec le demandeur principal sélectionné pour élaborer un accord de contribution, sur la base des activités proposées. Une fois l'accord conclu, le demandeur principal devient le bénéficiaire initial du financement et les organisations partenaires deviennent les bénéficiaires finaux en vertu de l'accord. L'accord énoncera les modalités de la contribution, y compris les obligations des deux parties et les conditions de paiement. Ces modalités doivent également être reflétées dans les accords signés entre le bénéficiaire initial et les bénéficiaires finaux.

Le montant du financement sera déterminé en fonction du coût total admissible de la proposition, ainsi que des autres sources de financement.

Les demandeurs doivent noter que tant qu'un accord écrit n'a pas été signé par les deux parties, le MDN n'a aucun engagement ni aucune obligation de verser une contribution financière à une proposition. Les dépenses engagées ou payées par les demandeurs avant la signature d'un tel accord de contribution ne sont pas admissibles.

Toutes les propositions financées seront annoncées sur le site web IDEeS.

10. Considérations permanentes pour le CSID

10.1 Loi sur le ministère du Conseil exécutif (M-30) pour les demandeurs du Québec

La Loi sur le ministère du Conseil exécutif (M-30) peut s'appliquer à un demandeur qui est un organisme municipal, un organisme scolaire ou un organisme situé dans la province de Québec. Ces demandeurs devront remplir un formulaire d'information supplémentaire et, s'ils sont assujettis aux exigences de la Loi, obtenir l'autorisation et l'approbation écrites du gouvernement du Québec avant la signature de toute entente de contribution.

10.2 Base des paiements de contribution

L'exercice financier du gouvernement du Canada s'étend du 1er avril au 31 mars. L'accord de contribution précisera les dates de début et de fin des coûts admissibles, ainsi que les documents requis à l'appui des demandes de paiement.

Les paiements de contribution seront effectués après réception et approbation des rapports financiers décrivant les coûts admissibles réels engagés, signés par le directeur financier du bénéficiaire ou un autre agent dûment autorisé. Les paiements seront liés à des étapes mesurables et prédéfinies, telles qu'énoncées dans l'accord de contribution.

À la demande du bénéficiaire, des paiements anticipés peuvent être autorisés, sous réserve d'une évaluation des besoins financiers, du niveau de risque et des besoins de trésorerie. Afin d'assurer une surveillance financière appropriée, une retenue raisonnable, proportionnelle au risque des activités financées, peut être appliquée aux paiements anticipés et aux paiements échelonnés. Les retenues seront libérées une fois que les conditions de l'accord de contribution auront été remplies.

Les bénéficiaires peuvent être tenus de présenter les rapports financiers suivants, comme spécifié dans l'accord de contribution :

- Des rapports prévisionnels, estimant les dépenses admissibles qui seront engagées au cours de chaque exercice financier ; et
- Des rapports réels, résumant les dépenses admissibles engagées et payées au cours de la période considérée.

Les paiements anticipés ne peuvent être utilisés que pour couvrir les coûts admissibles (voir l'annexe C – Coûts admissibles et non admissibles). **Les bénéficiaires initiaux sont tenus de dépenser tous les fonds reçus au cours de l'exercice financier pour lequel ils ont été versés.** Tout paiement anticipé non dépensé peut être considéré comme un trop-perçu et traité conformément aux dispositions de l'accord de contribution relatives aux trop-perçus, y compris le remboursement ou la réduction du montant de la contribution, majoré des intérêts applicables.

Les bénéficiaires doivent conserver les pièces justificatives et être prêts à fournir des documents à l'appui de toutes les dépenses admissibles engagées.

Le paiement final ne sera effectué qu'une fois que toutes les activités convenues auront été réalisées et jugées acceptables par le MDN.

10.3 Redistribution des fonds

L'approbation du MDN est requise avant la redistribution des fonds par un bénéficiaire à une ou plusieurs personnes ou entités.

Les dispositions de l'accord de contribution tiendront compte des exigences de la Politique sur les paiements de transfert du Conseil du Trésor et des modalités du programme. Ces modalités doivent également être reflétées dans les accords signés entre le bénéficiaire initial et les bénéficiaires finaux.

Si un bénéficiaire initial redistribue des fonds à un ou plusieurs bénéficiaires finaux :

- Le bénéficiaire initial est libre de choisir les bénéficiaires finaux, avec un minimum d'orientation de la part du MDN, et n'agira pas à titre d'agent du gouvernement dans le cadre de la distribution des fonds;
- L'accord de contribution du bénéficiaire initial tiendra compte des dispositions énoncées à l'annexe G (27 à 34) de la [Directive sur les paiements de transfert](#);
- Les bénéficiaires finaux qui reçoivent des fonds redistribués doivent être des bénéficiaires admissibles approuvés et doivent utiliser les fonds pour le type et la nature des coûts admissibles tels que définis à l'annexe C – Coûts admissibles et non admissibles.

10.4 Sécurité de la recherche

En mars 2021, le gouvernement du Canada a publié une [déclaration de politique sur la sécurité de la recherche](#) encourageant tous les membres de la communauté de la recherche, y compris les universités, le secteur privé et le gouvernement, à prendre des précautions supplémentaires pour protéger la sécurité de la recherche, la propriété intellectuelle et le développement des connaissances. Dans le cadre du présent appel de propositions, les bénéficiaires sont tenus d'identifier, d'évaluer et d'atténuer activement les risques pour la sécurité de la recherche d'une manière proportionnée à la sensibilité des activités entreprises, aux informations concernées et à la composition des partenaires proposés.

Les risques liés à la sécurité de la recherche peuvent inclure, sans s'y limiter, l'ingérence étrangère, l'accès non autorisé à des informations sensibles, l'utilisation abusive des résultats de la recherche et la compromission de la propriété intellectuelle ou du savoir-faire. Ces risques doivent être pris en compte tout au long du cycle de vie des activités du CSID, y compris la sélection des partenaires, l'accès aux données, l'accès du personnel, les installations et les flux d'informations.

Les demandeurs ne sont pas tenus d'éliminer tous les risques ni de mener uniquement des recherches classifiées. Ils doivent plutôt démontrer qu'ils comprennent les risques liés à la sécurité de la recherche et décrire des mesures d'atténuation raisonnables et adaptées à l'objectif visé.

Le Canada élabore actuellement des lignes directrices visant à intégrer les considérations de sécurité nationale dans l'évaluation et le financement des projets de recherche et des partenariats. Dans l'intervalle, les bénéficiaires sont tenus de faire preuve de diligence raisonnable et de mettre en œuvre des mesures d'atténuation proportionnées aux risques identifiés, plutôt que de se fier à des directives futures.

Lorsqu'elles seront disponibles, les lignes directrices devraient être intégrées au processus d'évaluation de diligence raisonnable entrepris par le MDN à l'appui des initiatives de recherche et développement. Entre-temps, les bénéficiaires sont encouragés à collaborer pour cerner et atténuer les risques potentiels pour la sécurité en utilisant les outils existants disponibles sur le portail [Protégez votre recherche](#) et dans le cadre des ateliers [de Science en sécurité](#). Les bénéficiaires doivent effectuer un examen cohérent et approprié

de diligence raisonnable des risques potentiels pour la sécurité des activités de recherche et mettre en place des mesures opportunes pour atténuer ces risques de manière appropriée.

Le MDN peut examiner les activités proposées pour des raisons de sécurité nationale afin de s'assurer que tous les risques pour la sécurité nationale sont identifiés et traités. Le MDN se réserve le droit de demander des informations supplémentaires, de collaborer avec les bénéficiaires sur les mesures d'atténuation des risques ou d'appliquer des conditions appropriées dans le cadre de l'accord de contribution, si nécessaire, afin de traiter les risques identifiés en matière de sécurité de la recherche. Conformément aux lignes directrices en matière de sécurité de la recherche, il peut être nécessaire de partager ces informations avec les ministères et organismes du gouvernement du Canada aux fins de l'évaluation des risques liés à la sécurité de la recherche.

Plan de sécurité de la recherche obligatoire

Les demandeurs doivent soumettre un **plan de sécurité de la recherche** dans le cadre de leur proposition (voir la partie 6 du formulaire de proposition). Le plan doit décrire :

- Le profil de risque pour la sécurité de la recherche des activités proposées ;
- Les mesures mises en place pour atténuer les risques identifiés ;
- La manière dont les données, les connaissances et les résultats de la recherche seront protégés et gérés ;
- La manière dont les partenariats et les collaborations sont gérés du point de vue de la sécurité.

Le [guide à l'intention des organismes de recherche et des bailleurs de fonds sur l'élaboration d'un plan de sécurité de la recherche](#) doit être consulté pour l'élaboration du plan. Le plan de sécurité de la recherche sera évalué selon une **approche proportionnelle et fondée sur les risques** et sera évalué dans le cadre des critères obligatoires (voir MC7 à l'annexe B).

10.5 Exigences en matière de rapports

Les exigences spécifiques en matière de rapports seront définies dans l'accord de contribution. Le modèle de prestation du CSID repose sur une collaboration active et un engagement continu. Chaque CSID se verra attribuer un **responsable BOREALIS CSID**, un expert en la matière du MDN qui travaillera en étroite collaboration et de manière continue avec le bénéficiaire afin de suivre les progrès, de soutenir la prestation et d'assurer l'alignement avec les priorités en matière de défense et de sécurité. Le responsable CSID servira de point de contact principal entre le CSID et la communauté de la défense et de la sécurité du gouvernement du Canada.

Des interactions régulières au niveau opérationnel entre le bénéficiaire et le responsable du CSID BOREALIS seront mises en place afin de permettre l'identification rapide des problèmes, la coordination et la prise de décisions tout au long de la période d'exécution.

En plus de cet engagement continu, le MDN exigera du bénéficiaire qu'il soumette des rapports d'étape officiels afin de faciliter la supervision et la reddition de comptes du programme. Au minimum, les bénéficiaires devront fournir :

- Trois (3) rapports d'étape par exercice financier – 1 oral et 2 écrits. Voici un exemple des informations demandées dans les rapports d'étape :
 - État d'avancement des activités et progrès réalisés par rapport aux objectifs et aux étapes clés du CSID

- Progrès réalisés dans la sécurisation des installations physiques et/ou numériques, le cas échéant
- Résumé des progrès techniques, opérationnels ou d'intégration rendus possibles grâce au CSID
- Description des activités d'expérimentation, d'essai, d'intégration ou de validation menées
- Nature et étendue de la collaboration avec le MDN/les FAC et d'autres intervenants dans le domaine de la défense et de la sécurité, y compris la participation des utilisateurs finaux visés
- Nombre et nature des partenariats et collaborations établis ou maintenus
- Mobilisation de fonds, y compris des contributions supplémentaires en espèces ou en nature
- Soutien au personnel hautement qualifié et au développement des compétences
- Prévisions des besoins en trésorerie et rapport sur les dépenses/résultats réels (semestriel ou trimestriel).

Le MDN peut demander que d'autres indicateurs de mesure du rendement soient fournis.

10.6 Collaboration des CSID avec les intervenants du domaine de la défense et de la sécurité

Les CSID doivent fonctionner comme des environnements de collaboration active pour le ministère de la Défense nationale (MDN), les Forces armées canadiennes (FAC) et d'autres intervenants du domaine de la défense et de la sécurité.

Les CSID financés doivent être prêts à accueillir et à faire participer le personnel du MDN/des FAC dans le cadre des activités normales du carrefour, y compris la collaboration au niveau opérationnel, les visites sur place, les démonstrations, les expérimentations, les essais, l'intégration et les activités de validation, en fonction du domaine concerné et du contexte de sécurité.

Dans le cadre de cette attente, les CSID doivent être prêts à :

- Fournir l'accès aux installations et/ou aux environnements numériques des CSID au personnel du MDN/des FAC, sous réserve des exigences applicables en matière de sécurité et d'accès
- Démontrer comment la collaboration avec les acteurs de la défense et de la sécurité, y compris d'autres programmes d'innovation du gouvernement fédéral, est intégrée dans la gouvernance, les opérations et les activités du CSID
- Présenter les progrès réalisés dans la mise en place et l'exploitation d'environnements sécurisés, y compris les avancées en matière d'accréditation de sécurité, le cas échéant
- Mettre en évidence la manière dont les activités des CSID éclairent, soutiennent ou font progresser les missions de défense et de sécurité nationale

Lors de la planification de leurs activités et budgets proposés, les demandeurs doivent tenir compte des ressources et des efforts nécessaires pour soutenir une collaboration régulière avec les acteurs de la défense et de la sécurité, y compris la préparation et les activités de suivi associées à ces collaborations.

10.7 Activités de communication

Les activités de communication liées aux Carrefours sécurisés de l'innovation pour la défense (CSID) doivent être menées d'une manière appropriée au contexte de la défense et de la sécurité nationale, en tenant compte de la nature sensible des activités et des collaborations des CSID.

Les CSID peuvent entreprendre des activités de communication afin de favoriser la transparence, la sensibilisation des parties prenantes et l'engagement auprès des publics concernés, lorsque cela est approprié et conforme aux exigences en matière de sécurité. Ces activités peuvent inclure des documents

destinés au public, des présentations, des démonstrations ou d'autres communications liées aux opérations ou aux résultats des CSID.

Avant toute diffusion publique, publication ou communication externe découlant des activités des CSID, le demandeur principal doit fournir à BOREALIS un préavis et les documents pertinents, conformément à l'accord de contribution. Cet examen vise à évaluer si les communications proposées peuvent contenir des informations sensibles ou préjudiciables à la sécurité nationale, et à déterminer si des mesures d'atténuation sont nécessaires.

Les communications publiques produites dans le cadre d'un CSID financé doivent mentionner la contribution du gouvernement du Canada, conformément aux directives fournies par BOREALIS, y compris l'utilisation d'éléments de reconnaissance et de marque approuvés. Le bénéficiaire doit faire des efforts raisonnables pour informer BOREALIS au moins quinze (15) jours ouvrables à l'avance de toute communication publique prévue, sauf indication contraire dans l'accord de contribution.

Dans la mesure du possible et lorsque cela est approprié, les communications peuvent être diffusées dans les deux langues officielles.

10.8 Propriété intellectuelle

Sauf indication contraire dans l'accord de contribution, la propriété intellectuelle (PI) générée dans le cadre des activités financées par le présent programme appartient à la partie qui la crée, qu'il s'agisse du bénéficiaire ou de tout partenaire participant.

Le bénéficiaire sera chargé de veiller à ce que des ententes appropriées en matière de PI soient en place entre toutes les organisations participantes, conformément à ce principe.

Le Canada peut, à sa seule discrétion, inclure dans l'accord de contribution une disposition exigeant que le bénéficiaire accorde au Canada, à perpétuité, une licence non exclusive, irrévocable, libre de droits et mondiale, lui permettant d'utiliser ou de faire utiliser la propriété intellectuelle à des fins gouvernementales. Cette licence permet au Canada de faire tout ce qu'il pourrait faire s'il était propriétaire de la PI, à l'exception de l'exploiter commercialement ou d'en transférer ou céder la propriété.

10.9 Conflit d'intérêts

Le bénéficiaire et tous les partenaires participants sont tenus d'identifier, de gérer et d'atténuer tout conflit d'intérêts réel, potentiel ou perçu, conformément à leurs politiques organisationnelles respectives et aux lois et règlements applicables.

S'il est sélectionné pour recevoir un financement, le programme peut demander des documents démontrant que le bénéficiaire et, le cas échéant, les partenaires participants sont conscients et ont pris en considération tout conflit d'intérêts réel, potentiel ou perçu, conformément à leurs lignes directrices internes en matière de conflits d'intérêts ou à leurs cadres de gouvernance.

L'accord de contribution comprendra des dispositions relatives aux conflits d'intérêts exigeant que le bénéficiaire informe rapidement le MDN de tout conflit d'intérêts réel, potentiel ou perçu survenant au cours de la période de financement, et qu'il prenne les mesures appropriées pour résoudre ces conflits à la satisfaction du MDN.

10.10 Droits de vérification

Le bénéficiaire doit :

- Tenir des comptes et des registres appropriés concernant les activités financées, pendant au moins six (6) ans après la date d'achèvement de l'accord ;
- Permettre aux représentants du gouvernement du Canada de vérifier, d'inspecter et de faire des copies de ces comptes et registres à tout moment raisonnable, jusqu'à six (6) ans après la date d'achèvement de l'accord ;
- Autoriser les représentants autorisés du gouvernement du Canada à vérifier et à inspecter le CSID admissible et les installations connexes ;
- Fournir aux représentants autorisés du gouvernement du Canada les renseignements qu'ils peuvent raisonnablement exiger de temps à autre en ce qui concerne les documents mentionnés dans les présentes ;
- Rembourser rapidement au MDN tout paiement excédentaire de la contribution révélé par une vérification, au plus tard trente (30) jours civils après la date de l'avis du Canada.

Annexe A – Énoncé du défi

Carrefours sécurisés de l'innovation pour la défense – Systèmes sans pilote (UxS) et technologie quantique

Les organismes canadiens chargés de la défense et de la sécurité nationale évoluent dans un environnement caractérisé par des changements technologiques rapides, une complexité croissante des systèmes et des exigences accrues en matière de sécurité. Les technologies de pointe, telles que les systèmes sans pilote (UxS) et la technologie quantique, devraient avoir une incidence importante sur les opérations futures de défense et de sécurité. Cependant, bien qu'il existe des environnements d'essai et d'expérimentation, rares sont ceux qui conviennent aux travaux impliquant des applications militaires sensibles. Malgré l'innovation rapide dans les secteurs commercial et de la recherche, l'absence de conditions fiables pour le développement, l'intégration et la démonstration limite la traduction des technologies prometteuses des UxS et de la technologie quantique en capacités opérationnelles pertinentes. Sans mécanismes permettant une expérimentation contrôlée et une collaboration fiable au niveau de classification requis, le Canada risque de retarder l'adoption de ces technologies et de réduire son avantage opérationnel à mesure que celles-ci mûrissent à l'échelle mondiale. Ce défi vise à combler cette lacune en créant des conditions propices au développement, à l'intégration et à la démonstration des technologies des UxS et de la technologie quantique à des fins de défense.

Ce que BOREALIS offre

Environ 50 millions de dollars, répartis entre deux volets (UxS et quantique), fournis par le biais du programme Innovation pour la défense, l'excellence et la sécurité (IDEeS) sous forme de contributions non remboursables, afin de soutenir la création et la mise à niveau sécuritaire d'installations existantes en tant que CSID dans les domaines UxS ou quantique et de faire progresser l'innovation, ainsi que de stimuler la collaboration.

Ce qu'apportent les innovateurs

Un consortium composé d'au moins deux partenaires éligibles, apportant des installations existantes, des liens solides avec les écosystèmes d'innovation locaux et la capacité de mener à bien un programme cohérent de recherche et développement dans les domaines des systèmes sans pilote (UxS) ou de la technologie quantique, développé conjointement avec les partenaires du consortium et leur écosystème, comme défini dans les énoncés de défi pour chaque volet ci-dessous. Les consortiums sont tenus de sécuriser et d'exploiter ces installations en tant que carrefour sécurisé de l'innovation pour la défense (CSID) et de tirer parti des partenariats entre l'industrie, le monde universitaire, le gouvernement et le secteur à but non lucratif pour soutenir la R&D collaborative, l'échange de connaissances et le progrès technologique en accord avec les besoins en matière de défense et de sécurité.

Volet Systèmes sans pilote (UxS)

Le défi

Les systèmes sans pilote et les contre-systèmes sans pilote (UxS et c-UxS) transforment rapidement la nature des opérations militaires modernes. Si la recherche et l'innovation commerciales et universitaires dans ce domaine progressent rapidement, il subsiste des lacunes importantes dans la capacité à

développer, intégrer et perfectionner des technologies UxS et c-UxS qui soient résilientes, interopérables et efficaces dans des environnements de défense et de sécurité contestés. Le CSID vise à accélérer la transition des technologies UxS et c-UxS prometteuses vers des capacités pertinentes pour la défense en permettant des activités ciblées de recherche, de développement, d'intégration et de démonstration, alignées sur l'évolution des besoins opérationnels dans un environnement sécurisé.

Contexte

La disponibilité, l'accessibilité financière et les capacités croissantes des plateformes UxS présentent des opportunités et des défis pour le MDN/les FAC et les partenaires de sécurité nationale. Les homologues internationaux recherchent de plus en plus une combinaison de plateformes haut de gamme, survivable et sans équipage, et de systèmes plus nombreux et moins coûteux, s'éloignant de la dépendance exclusive à l'égard des plateformes avec équipage pour se tourner vers des réseaux intégrés de systèmes autonomes et semi-autonomes capables de fonctionner dans des environnements contestés, dégradés et difficiles. Ces tendances concernent les applications aériennes, terrestres et multi-domaines. En parallèle, les progrès rapides réalisés par des adversaires potentiels risquent de dépasser les capacités c-UxS existantes. Pour relever ces défis, il est nécessaire de coordonner la recherche et le développement dans plusieurs domaines et axes techniques, notamment les systèmes aériens et terrestres sans pilote.

Résultats attendus

Le CSID UxS devrait renforcer les solutions fabriquées au Canada grâce à des chaînes d'approvisionnement souveraines et évolutives pour le MDN/les FAC et d'autres partenaires en matière de sécurité, en permettant et en menant des projets de recherche et développement, en mettant l'accent sur les projets de niveaux de maturité technologique 4 à 9, afin de perfectionner, de valider, de tester et d'intégrer les technologies UxS et c-UxS dans des capacités opérationnelles pertinentes, favorisant ainsi une plus grande résilience face à l'évolution des capacités adverses. Les domaines d'intérêt peuvent inclure, sans s'y limiter :

- **Domination du spectre** – Garantir la liberté d'opérer à travers ou sans le spectre électromagnétique, soutenir les objectifs UxS et priver les adversaires de la même capacité. Cela comprend les progrès en matière de guerre électronique, la résilience des commandes et contrôles, ainsi que des liaisons de données et des réseaux robustes.
- **Connaissance du domaine** – Systèmes multi capteurs permettant la détection distribuée, les systèmes embarqués de détection et d'évitement (DAA), la conscience situationnelle, la coordination multi-UxS, l'acquisition et le suivi de cibles grâce à la fusion avancée de capteurs tels que, sans s'y limiter, les réseaux acoustiques, les capteurs électro-optiques, les télémètres et désignateurs laser et les systèmes de détection des radiofréquences.
- **Persistance** – Maximiser le temps de fonctionnement, la portée, la vitesse, la charge utile et la flexibilité opérationnelle grâce à des options telles que la propulsion hybride-électrique, les systèmes d'alimentation et d'énergie à haute densité, le poids, le routage et d'autres optimisations ; augmenter la résilience des UxS dans des conditions environnementales difficiles, telles que l'Arctique ; et soutenir les opérations dans des environnements contestés avec des infrastructures de soutien limitées.
- **Interopérabilité** – Garantir que les UxS fonctionnent avec des niveaux élevés de sécurité, de fiabilité et de performance, y compris au sein d'équipes homme-machine et aux côtés de plateformes habitées, ainsi que sur toute une gamme d'infrastructures terrestres et aériennes, de charges utiles et de systèmes de lancement et de récupération. Cela comprend l'intégration avec

les cadres de gestion de l'espace aérien et au sol pertinents, la recherche sur les facteurs humains, l'assurance de l'autonomie et les tests de fiabilité.

- **Autonomie, aide à la décision et effets sur le champ de bataille** – Approches permettant des comportements autonomes fiables, des fonctions d'aide à la décision et des effets autonomes dans tous les domaines opérationnels. Cela comprend des interfaces homme-machine avancées, une autonomie au niveau de la mission, une prise de décision adaptative dans des environnements dégradés ou contestés, et des effets sur le champ de bataille rendus possibles par l'autonomie (y compris des actions cinétiques et non cinétiques) afin de contribuer à compenser les pénuries de personnel auxquelles sont confrontées les FAC et les partenaires de sécurité nationale. Une autonomie fiable nécessite le développement de cadres validés en matière de confiance, de sécurité et d'assurance qui garantissent que les systèmes autonomes peuvent produire de manière fiable des effets critiques pour la mission.
- **C2 multi-UxS et effets coordonnés** – La multiplication future des forces basée sur les UxS nécessite des solutions permettant une collaboration homme-machine efficace, de sorte que les opérateurs puissent intuitivement et efficacement commander et contrôler de grands ensembles de systèmes autonomes hétérogènes (1: plusieurs) grâce à des instructions compréhensibles par l'homme et basées sur des objectifs. Ces solutions doivent permettre aux UxS hétérogènes d'interpréter les intentions humaines, de planifier et de diriger des activités individuellement ou collectivement, de coordonner leurs actions de manière collaborative entre les différents domaines et d'agir de manière autonome sur le champ de bataille. Les concepts opérationnels émergents s'appuient de plus en plus sur la collaboration de plusieurs UxS hétérogènes afin de produire des effets combinés (par exemple, des UAS à longue endurance fournissant des guidages de ciblage pour les munitions FPV ou une aide à la navigation pour les UGV). Pour obtenir ces effets coordonnés, il est nécessaire de faire progresser les algorithmes, les interfaces homme-machine et les technologies de communication pour les opérations coopératives sans équipage.
- **Fabrication avancée** – Méthodes de production souveraines et évolutives avancées pour optimiser les performances du système grâce à la résilience de la chaîne d'approvisionnement, au volume de production et à la rapidité de reconception. Le système de conception et de production doit garantir la redondance de l'approvisionnement en pièces, s'adapter aux changements importants de la demande de production, répondre rapidement aux changements de conception dictés par le théâtre d'opérations et permettre une réparation facile des UxS et c-UxS en théâtre d'opérations.

Volet quantique

Le défi

Les technologies quantiques ont le potentiel de modifier fondamentalement la détection, les communications, l'informatique et la navigation dans les contextes de défense et de sécurité. Bien que des progrès significatifs soient réalisés à l'échelle mondiale, les capacités quantiques pertinentes pour la défense se heurtent à des obstacles uniques liés à la sensibilité, à la sécurité, à l'intégration et aux essais. Ce défi vise à accélérer la maturation et l'application des technologies quantiques qui sont essentielles à la défense et à la sécurité nationale en permettant des activités de recherche, de développement, d'intégration et de démonstration ciblées dans des environnements fiables.

Contexte

Les technologies quantiques sont une catégorie émergente et hautement sensible de technologies qui ont des implications importantes pour la défense et la sécurité. Alors que la concurrence géopolitique dans le domaine quantique s'intensifie, le Canada doit considérer les capacités quantiques comme un atout stratégique et souverain, essentiel au maintien de l'avantage opérationnel et à la protection des systèmes critiques de défense et de sécurité. Parallèlement, de nombreuses technologies quantiques prometteuses se heurtent à des difficultés pour passer de la recherche en laboratoire à des applications pertinentes pour la défense, en particulier lorsque des installations sécurisées, une intégration au niveau du système et des essais réalistes sont nécessaires.

Résultats attendus

Le CSID quantique devrait renforcer la posture du Canada en matière de défense et de sécurité en faisant progresser les technologies quantiques vers une pertinence opérationnelle et en réduisant le risque de surprise technologique. Les propositions devraient contribuer à la maturation des capacités quantiques pertinentes pour la défense grâce à des activités telles que l'intégration des systèmes, la robustification, les essais et l'évaluation (y compris les essais sur le terrain, le cas échéant) et la démonstration, lorsque celles-ci sont nécessaires pour répondre aux besoins en matière de défense et de sécurité. Les domaines d'intérêt peuvent inclure, sans s'y limiter :

- **Détection quantique** – Technologies radar, lidar et d'imagerie améliorées par la technologie quantique qui offrent une sensibilité, une précision, une résilience, une discrétion ou des effets de détection qualitativement nouveaux, dépassant ce qui est réalisable avec les approches de détection conventionnelles, et qui facilitent la détection et la connaissance de la situation dans des environnements contestés ou interdits.
- **Positionnement, navigation et synchronisation alternatifs (PNT)** – Approches de détection et de synchronisation quantiques qui facilitent la navigation ou la distribution temporelle dans des environnements où le GNSS est défaillant, dégradé ou contesté, y compris l'intégration avec les plateformes, les systèmes et les flux de travail opérationnels existants.
- **Informatique et algorithmes quantiques** – Approches informatiques quantiques et hybrides quantiques-classiques, y compris les algorithmes, les outils logiciels et les flux de travail (y compris l'intégration de l'informatique quantique et de l'IA), qui permettent des tâches d'analyse, de modélisation, de simulation, d'optimisation et d'aide à la décision pertinentes pour la défense, ainsi que la conception et la découverte rapides de matériaux, de dispositifs ou de contre-mesures médicales pertinents pour la défense, et leur validation par la synthèse, les tests et la démonstration, le cas échéant.
- **Communications et réseaux quantiques** – Technologies et architectures de réseau qui appuient les communications et les réseaux quantiques, y compris la distribution de clés quantiques et l'intégration de systèmes de communication quantiques terrestres, aériens et spatiaux.

Annexe B – Critères d'évaluation

Les demandeurs doivent remplir le formulaire de proposition CSID de manière suffisamment détaillée pour permettre au Canada d'évaluer la proposition par rapport aux critères d'évaluation établis. Les informations fournies doivent démontrer clairement comment la proposition répond à chaque critère.

Les propositions seront évaluées à l'aide de critères obligatoires (MC) et de critères pondérés (PRC).

Pour être admissibles au financement, les propositions doivent satisfaire à tous les critères obligatoires. Il incombe au demandeur de démontrer que la proposition répond clairement à chaque critère.

Critères obligatoires (MC)

Critères	Matrice d'évaluation (réussite/échec)
MC1 – Admissibilité du demandeur	Réussite : Le demandeur doit être une personne morale dûment constituée en vertu des lois fédérales ou provinciales du Canada et valablement existante au Canada, notamment : • Les universités canadiennes et autres établissements d'enseignement postsecondaire agréés au Canada • Les organisations ou associations canadiennes à but non lucratif constituées en société • Les sociétés, organisations ou associations canadiennes à but lucratif constituées en société Non admissible : Le demandeur n'est pas une personne morale dûment constituée en vertu des lois fédérales ou provinciales du Canada et valablement existante au Canada, comme indiqué ci-dessus ; ou est un ministère fédéral, un organisme fédéral, une société d'État ou un organisme gouvernemental provincial/territorial ou municipal.
MC2 – Composition minimale du partenariat	Réussite : La proposition doit identifier, au minimum, des partenaires provenant d'au moins deux (2) organisations et/ou institutions distinctes admissibles; et le rôle de chaque partenaire est décrit de manière générale, démontrant comment chacun contribue à la réalisation des objectifs du carrefour sécurisé de l'innovation pour la défense (CSID) proposé. Échec : Un ou plusieurs partenaires requis ne sont pas identifiés ; ou les partenaires sont identifiés uniquement par leur nom, sans description de leur rôle dans le CSID proposé.
MC3 – Alignement sur les objectifs du CSID	Admis : La proposition doit répondre à l'intention fondamentale de l'appel à propositions CSID, dont l'objectif principal est la recherche, le développement et/ou l'expérimentation dans le domaine de la défense ou de la sécurité, et doit s'aligner sur un ou plusieurs domaines prioritaires identifiés dans l'appel (systèmes quantiques ou sans pilote).

	Échec : La proposition ne répond pas aux objectifs du CSID, est hors sujet ou est principalement de nature commerciale, civile ou infrastructurelle.
MC4 – Activités éligibles, coûts et limites de financement	Admissible : Les activités proposées doivent être éligibles dans le cadre de l'appel à propositions CSID, et le budget proposé doit respecter toutes les limites de financement, notamment : • Les dépenses d'investissement ne dépassant pas 50 % du total des coûts éligibles • Les frais administratifs/généraux ne dépassant pas 15 % du total des coûts éligibles Non admissible : La proposition comprend des activités ou des coûts non éligibles, ou dépasse une ou plusieurs limites de financement.
MC5 – Identification et préparation des infrastructures physiques	Réussite : La proposition doit identifier l'infrastructure physique qui sera utilisée pour le CSID et inclure un plan de haut niveau démontrant que l'infrastructure existe et/ou peut être mise à disposition, équipée de manière appropriée et sécurisée pendant la période de financement. Échec : La proposition n'identifie pas d'infrastructure physique, ou l'infrastructure est purement conceptuelle.
MC6 – Faisabilité pendant la période de financement	Réussite : La proposition doit inclure un plan de travail de haut niveau démontrant que les principales activités de recherche, de développement, d'expérimentation et de coordination peuvent être achevées avant le 31 mars 2028. Échec : Aucun plan de travail n'est fourni, ou les activités du centre dépassent clairement la période de financement sans justification.
MC7 – Plan de sécurité de la recherche	Admis : La proposition comprend un plan de sécurité de la recherche de haut niveau qui est manifestement conforme aux lignes directrices du gouvernement du Canada à l'intention des organismes de recherche et des bailleurs de fonds sur l'élaboration d'un plan de sécurité de la recherche. Échec : La proposition ne comprend pas de plan de sécurité de la recherche, ou le plan ne traite pas des éléments définis par le gouvernement fédéral dans les Lignes directrices à l'intention des organismes de recherche et des bailleurs de fonds sur l'élaboration d'un plan de sécurité de la recherche.

Critères notés sur une échelle de points (PRC)

Une échelle de points est utilisée pour évaluer les critères notés. Si la proposition fournit des informations insuffisantes ou aucune information pour l'un des critères, elle peut se voir attribuer une note insuffisante ou zéro point.

Échelle de notation :

Insuffisant : 0 point

Médiocre : 1 point

Passable : 3 points

Bon : 6 points

Excellent : 10 points

Collectivement, les critères notés évaluent la pertinence en matière de défense, la qualité de la prestation, la collaboration, la mise en place d'infrastructures, le rapport qualité-prix, l'inclusivité et la durabilité des capacités CSID.

Critères	Critères d'évaluation
PRC1 - Pertinence pour la défense et la sécurité	Les demandeurs doivent clairement démontrer la pertinence du CSID proposé pour la défense et/ou la sécurité. Cela implique de définir clairement le problème de défense ou de sécurité et le contexte d'utilisation prévu, de démontrer que les activités de R&D et d'expérimentation proposées sont étroitement liées à ce problème, de montrer leur pertinence par rapport au(x) domaine(s) prioritaire(s) identifié(s) dans l'appel à propositions et de décrire un cheminement plausible entre les activités de R&D et l'utilisation à des fins de défense, la mise en œuvre de l'expérimentation ou l'adoption de la capacité.
PRC2 - Qualité et cohérence du programme de R&D	Les demandeurs doivent présenter un programme de R&D et d'expérimentation cohérent et bien structuré. Cela implique des objectifs clairement définis et mesurables, un enchaînement logique des activités, des résultats ou des livrables définis, l'identification des principaux risques techniques et des stratégies d'atténuation, ainsi qu'une portée ambitieuse mais crédible compte tenu du financement, des installations et du calendrier.
PRC3 - Capacité de livraison, de gouvernance et d'exécution	Les demandeurs doivent démontrer une approche de mise en œuvre et de gouvernance capable de faire fonctionner un carrefour sécurisé de l'innovation pour la défense et d'exécuter plusieurs efforts de R&D simultanés. Cela comprend des structures décisionnelles claires, des rôles et des responsabilités bien définis entre les partenaires, une approche de gestion opérationnelle crédible et la preuve d'une expérience pertinente dans la mise en œuvre d'initiatives complexes impliquant plusieurs partenaires. Cela comprend également l'identification des principaux risques liés au calendrier et des stratégies d'atténuation, dans le cadre d'un plan crédible visant à dépenser la totalité du budget proposé dans les délais prévus.

PRC4 - Modèle de collaboration et intégration des partenaires	Les demandeurs doivent démontrer une intégration significative des partenaires dans l'exécution des activités de R&D et d'expérimentation. Cela implique de montrer que tous les partenaires sont intégrés dans des rôles de prestation, que les mécanismes de collaboration permettent un transfert efficace des connaissances et que les dispositions relatives à la propriété intellectuelle, aux données et à l'accès ont été prises en compte à un niveau approprié pour la portée des travaux.
PRC5 - Qualité de l'infrastructure et de la sécurité	Les demandeurs doivent démontrer que l'infrastructure et la sécurité proposées sont bien adaptées aux activités de R&D et d'expérimentation. Cela implique notamment la pertinence des installations, la crédibilité de toute évolution progressive de la sécurité et la capacité de l'infrastructure à prendre en charge une expérimentation agile et multi-utilisateurs.
PRC6 - Rapport qualité-prix et co-investissement	Les demandeurs doivent démontrer que le budget proposé présente un bon rapport qualité-prix et qu'il est adapté à l'obtention des résultats de R&D et d'expérimentation. Cela inclut la hiérarchisation des activités de R&D, la justification des dépenses d'infrastructure, l'allocation efficace des ressources entre les partenaires et, le cas échéant, un co-investissement crédible et complémentaire qui renforce la proposition.
PRC7 - Durabilité	Les demandeurs doivent identifier les capacités du CSID qui devraient avoir une valeur au-delà de la période de financement et décrire une approche crédible pour maintenir ou faire évoluer ces capacités après la fin du financement. Cela comprend l'alignement de l'utilisation post-financement avec les objectifs de défense et de sécurité.
PRC8 - ACS+ et accès inclusif	Les demandeurs doivent décrire comment les considérations GBA+ ont été prises en compte de manière proportionnée à la portée de la proposition. Cela comprend la prise en compte de la participation inclusive et de l'accès équitable aux capacités CSID, y compris la manière dont les acteurs éligibles de l'industrie, du monde universitaire et d'autres parties prenantes peuvent raisonnablement accéder et participer aux activités CSID, conformément aux exigences en matière de sécurité, de sûreté et d'exploitation.

Annexe C – Coûts admissibles et non admissibles

Les coûts admissibles sont limités aux catégories suivantes.

1. Salaires et avantages sociaux

Les salaires et avantages sociaux sont éligibles s'ils sont directement liés aux activités du CSID, y compris la gestion de projet, et reflètent les coûts exacts associés au paiement des salaires et avantages sociaux.

- Salaires : ne doivent pas dépasser 250 000 dollars par équivalent temps plein (hors avantages sociaux). Ce plafond s'applique à tous les postes (y compris les contrats de travail) et est calculé au prorata du temps de travail par rapport à l'équivalent temps plein.
- Avantages sociaux : ne doivent pas dépasser 25 % des salaires par équivalent temps plein.

Les avantages sociaux sont définis comme les coûts salariaux payés par l'employeur et peuvent inclure les éléments suivants :

- Part patronale du RPC/RRQ
- Part patronale de l'assurance-emploi (AE)
- Part patronale de l'assurance collective
- Cotisations de retraite de l'employeur

2. Services professionnels (fournis par des tiers non affiliés au bénéficiaire)

Les services professionnels admissibles comprennent les travaux effectués par des experts externes, des consultants ou des fournisseurs de services qui sont engagés spécifiquement pour fournir des connaissances spécialisées, une expertise ou des services techniques directement nécessaires à la réalisation du projet approuvé.

Il incombe au bénéficiaire de s'assurer que tous les coûts engagés auprès des fournisseurs de services contractuels sont admissibles. Sur demande, les bénéficiaires fourniront au MDN une copie des contrats de services conclus dans le cadre du CSID.

L'accord de contribution du CSID ne doit pas être utilisé ou reproduit pour conclure des contrats avec d'autres parties. Le contrat du bénéficiaire doit détailler les activités et les résultats à atteindre dans le cadre de ce contrat, les coûts et les livrables.

Remarque : les services professionnels spécifiques liés à l'aménagement des installations existantes sont considérés comme relevant de la sous-catégorie 4 « *Dépenses en capital (équipement et installations)* » et sont donc inclus dans le plafond de 50 % du total des coûts admissibles de la proposition qui peuvent être consacrés à l'aménagement des installations existantes.

3. Dépenses de R&D

Les dépenses de R&D admissibles comprennent les coûts directement attribuables à la conduite de recherches fondamentales et appliquées visant à relever les défis en matière de défense et de sécurité nationale identifiés dans le plan de R&D du CSID.

Les dépenses de R&D peuvent inclure, sans s'y limiter :

- Matériaux et fournitures : petits composants de systèmes, composants électroniques et tout autre matériel intégré dans des prototypes ou consommé au cours des activités de R&D. Cela comprend également les stocks de matériaux utilisés pour fabriquer des composants sur place.
- Prototypage : dépenses liées au développement de prototypes et de systèmes de solutions, à la validation et à l'intégration, aux essais et à l'évaluation.
- Acquisition et analyse de données : coûts liés à la collecte de données, à l'acquisition des ensembles de données nécessaires, aux environnements de test, aux outils de modélisation et aux logiciels d'analyse requis pour soutenir les objectifs de R&D. Les coûts liés à l'accès à la documentation de recherche, telle que les revues scientifiques et les bases de données d'information, utilisée pour la mise en œuvre du plan de R&D du CSID sont admissibles dans cette sous-catégorie.
- Déplacements : frais de déplacement nécessaires à la conduite de recherches, à la collaboration avec les parties prenantes du MDN/FCA, à des essais sur le terrain ou à des examens techniques, lorsqu'ils sont directement liés aux activités de R&D. Les frais de déplacement doivent être engagés conformément à la directive sur les voyages du Conseil national mixte.

4. Dépenses en capital (équipement et installations)

Le matériel est défini comme tout article (ou ensemble d'articles interdépendants constituant un système) qui est utilisé en tout ou en partie pour la recherche proposée et qui remplit les trois conditions suivantes :

- 1) Bien matériels durables ;
- 2) Avoir une durée de vie utile de plus d'un an ; et
- 3) Un coût de 2 000 \$ ou plus.

Remarque : un article qui ne remplit pas les trois conditions énumérées ci-dessus peut être classé comme matériel et fournitures (voir 3. *Dépenses de R&D* ci-dessus).

Le bénéficiaire sera responsable d'obtenir la juste valeur de l'équipement au moment de l'achat.

Les coûts admissibles dans la sous-catégorie des installations comprennent les modifications, les mises à niveau et l'aménagement des installations existantes nécessaires pour permettre un travail collaboratif sécurisé jusqu'au niveau II (secret), tels que les améliorations de la sécurité physique, les contrôles d'accès, les salles sécurisées et les infrastructures de soutien.

- Les coûts doivent être directement liés à la mise en œuvre des activités CSID.
- Les coûts d'aménagement ne doivent pas dépasser 50 % du total des coûts admissibles approuvés.
- Les nouvelles constructions, y compris les ajouts aux bâtiments existants, ne sont pas admissibles.

5. Frais généraux administratifs

Les frais généraux administratifs sont des dépenses indirectes engagées par les bénéficiaires, qui sont nécessaires à la mise en place du CSID et/ou aux activités de recherche, mais qui ne peuvent être spécifiquement identifiées comme des coûts directs. Ces coûts sont liés à l'utilisation des ressources de l'organisation, qui peuvent inclure, sans s'y limiter :

- Le soutien administratif (par exemple, la comptabilité, la gestion des salaires, les réunions) ;
- Le soutien informatique ;
- Internet, téléphone, à l'exclusion des frais d'appels interurbains ;
- Utilisation de photocopieurs, de télécopieurs et d'autres équipements de bureau ;
- Utilisation des postes de travail existants, y compris le mobilier et l'équipement (par exemple, les ordinateurs, les scanners) ;
- Logiciels bureautiques courants (à l'exclusion des logiciels spécifiquement requis pour le projet) ;
- Adhésions et abonnements uniquement si nécessaire pour mener à bien les activités du projet ;
- Recrutement et formation du personnel ;
- Entretien courant du matériel de laboratoire et de terrain (par exemple, vidanges d'huile) ;
- Frais d'occupation et d'exploitation des bâtiments (c'est-à-dire utilisation de l'espace) ; et
- Entretien des installations.

Les frais généraux administratifs ne peuvent dépasser 15 % du total des dépenses admissibles (avant frais généraux).

6. Protection de la propriété intellectuelle

Les dépenses admissibles comprennent les coûts directement liés à la protection, à la sécurisation et à la gestion de la propriété intellectuelle découlant des activités financées.

Les coûts de propriété intellectuelle admissibles peuvent inclure, sans s'y limiter, **les coûts liés aux brevets** :

- Préparation et dépôt de brevets liés aux résultats du CSID.
- Frais de poursuite des brevets (par exemple, frais officiels de dépôt auprès des autorités gouvernementales).
- Recherches de brevets et évaluations de nouveauté.

Les coûts non admissibles comprennent, sans s'y limiter, les suivants :

- Les salaires et avantages sociaux des chercheurs qui reçoivent un salaire direct et continu par l'intermédiaire d'universités ou d'autres établissements d'enseignement supérieur ;
- Contributions en nature ;
- Formation ou perfectionnement professionnel, comme les cours d'informatique ou de langues ;
- L'achat de terrains ou de bâtiments ;
- Les frais liés au déménagement d'un laboratoire ;
- L'achat ou la location de véhicules privés/personnels, les frais d'entretien des véhicules ou les frais de « location » des véhicules appartenant à l'entreprise ;
- Les actifs et les biens d'équipement qui ne sont pas spécifiquement nécessaires à l'exécution des activités du CSID ;

- Les coûts normaux liés à la création d'une activité commerciale ;
- Les coûts liés aux activités considérées comme faisant partie des pratiques commerciales normales de tout bénéficiaire, telles que : les missions d'examen et d'audit, sauf si elles sont requises dans le contrat, les réunions du conseil d'administration, les assurances ;
- Amortissements ;
- Les intérêts ou frais de découvert et les frais de carte de crédit ;
- La partie remboursable de la TPS/TVH, des taxes sur la valeur ajoutée ou d'autres éléments pour lesquels un remboursement ou une remise est recevable ;
- Les frais de représentation, tels que la restauration, l'alcool, les divertissements, les honoraires, les cadeaux (par exemple, les cadeaux pour les conférenciers ou les animateurs) ;
- Frais de stationnement mensuels pour les véhicules, sauf si cela est spécifiquement requis pour le travail sur le terrain ;
- Coûts des vêtements courants ;
- Les frais d'adhésion, sauf s'ils sont spécifiquement requis pour l'exécution des activités financées et que les partenaires du CSID ne sont pas déjà membres ;
- Avantages sociaux discrétionnaires (p. ex. stationnement sur le lieu de travail, frais de déménagement pour les employés embauchés pour le CSID, prestations d'assurance-emploi supplémentaires pour les congés de maternité/paternité, récompenses et reconnaissance du personnel) ;
- Coûts des activités visant à influencer directement/faire pression sur les gouvernements ;
- Activités de marketing direct, de promotion commerciale ou de vulgarisation individuelle ;
- Les coûts liés à l'examen des thèses de maîtrise et de doctorat ; et
- Autres coûts non spécifiquement requis pour le CSID.