PROGRAMME DE RECHERCHE
DE L'ICSIA
AU CIFAR

APPEL DE PROPOSITIONS :

Projets Catalyseur sur la cybersécurité et les risques liés à l'IA agentique

CIFAR

Financé par le gouvernement du Canada | Canada

Table des matières

Possibilité de financement 3

Thèmes de recherche 4

IA agentique et contrôle des systèmes autonomes 4

Cybersécurité, déploiement de modèles à poids ouverts et risques systémiques 5

Admissibilité et modalités de financement 7

Volet A — Projets canadiens 7

Volets B — Projets en partenariat 7

Présentation des demandes 8

Calendrier 8

Exigences liées au projet 9

Critères de sélection 10

Utilisation de l'IA générative 10

Exigences de présentation de l'information 10

Possibilité de financement

Le Programme de recherche de l'ICSIA (Institut canadien de la sécurité de l'intelligence artificielle) au CIFAR a le plaisir de lancer un appel de propositions pour financer des projets Catalyseur en recherche fondamentale et appliquée sur la sécurité de l'IA. Ce financement vise à soutenir des projets audacieux à fort impact et des propositions hautement innovantes susceptibles de produire de vastes retombées dans ce domaine.

Le Programme de recherche de l'ICSIA au CIFAR dirige, de manière indépendante, la recherche multidisciplinaire au Canada sur les défis de sécurité que posent les systèmes d'IA avancés. Fer de lance de l'ICSIA, le Programme mobilise l'expertise canadienne en recherche sur l'intelligence artificielle pour approfondir les savoirs essentiels à la sécurité de l'IA.

Cet appel de propositions financera deux volets de recherche distincts : un **volet A**, pour les projets de chercheuses et chercheurs établis au Canada, et un **volet B** pour les projets internationaux admissibles. Les deux volets couvriront, pour une période maximale de deux ans, le salaire, les avantages sociaux et les frais de déplacement d'une chercheuse ou d'un chercheur postdoctoral. Les projets doivent porter sur les risques de l'IA agentique pour la sécurité et la société, ou sur les enjeux de cybersécurité connexes.

Dans le cadre du **volet B**, le Programme cofinancera, avec des organismes partenaires en Allemagne et en France, des projets novateurs en sécurité de l'IA menés par des équipes canado-allemandes ou canado-françaises.

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Le **CISPA** (Centre Helmholtz pour la sécurité de l'information), membre de l'Association Helmholtz, compte parmi les plus grands centres de recherche nationaux d'Allemagne. Il s'impose aujourd'hui comme un chef de file mondial en cybersécurité et en IA digne de confiance.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
Inria

L'Inria (Institut national de recherche en sciences et technologies du numérique), agence chargée des programmes numériques, soutient les stratégies nationales de recherche et d'innovation du gouvernement français dans ce domaine. Dans le cadre de l'initiative France 2030, il a lancé le programme Évaluation de l'IA pour établir la feuille de route scientifique de l'INESIA (Institut national pour l'évaluation et la sécurité de l'IA).

Thèmes de recherche

Cet appel de propositions porte sur deux enjeux majeurs et étroitement liés de la sécurité de l'IA : l'IA agentique et la cybersécurité. Les propositions doivent traiter de l'un ou l'autre de ces thèmes (ou les deux), selon une approche technique ou sociotechnique, et s'inscrire dans un ou plusieurs des axes suivants :

IA agentique et contrôle des systèmes autonomes

- **Mécanismes efficaces de supervision humaine :** Concevoir des cadres et des indicateurs pour évaluer et vérifier le respect des exigences de supervision humaine à chaque étape des processus de travail agentiques autonomes. Les projets peuvent notamment porter sur :
  - la mesure de l'efficacité de la supervision;
  - les données probantes axées sur les facteurs humains;
  - les stratégies pour prévenir la manipulation des indicateurs de performance.
- **Contrôle des systèmes hautement autonomes :** Mettre au point des méthodes robustes, des protocoles de confinement et des mécanismes de sécurité intégrée pour établir et maintenir le contrôle des systèmes agentiques, même en présence d'agents non coopératifs. Les projets peuvent notamment porter sur :
  - les mécanismes techniques (p. ex., confinement, exécution en environnement isolé, modèles de supervision);
  - les mécanismes non techniques (gouvernance, cadres de réglementation et d'octroi de licences, signalement des incidents);
  - les leçons tirées d'autres secteurs sensibles comme l'énergie nucléaire et l'aviation.

- **Transparence et interprétabilité des modèles :** Élaborer des méthodes pour auditer et encadrer le raisonnement et les décisions des systèmes agentiques. Les projets peuvent notamment porter sur :
  - les pistes d'audit des décisions et les traces de raisonnement des agents d'IA;
  - l'interprétabilité et les mécanismes de surveillance;
  - la conception de mécanismes sociotechniques de transparence et d'auditabilité tenant compte des compromis à faire en matière de protection des renseignements personnels, de sécurité et de respect de la propriété intellectuelle;
  - les enjeux de sécurité dans des secteurs sensibles comme la santé, les finances et les services publics.

Cybersécurité, déploiement de modèles à poids ouverts et risques systémiques

- **Cybersécurité et réduction des menaces systémiques :** Développer des solutions aux nouvelles vulnérabilités informatiques, aux menaces liées aux systèmes agentiques et aux risques systémiques du déploiement de systèmes d'IA avancés. Les projets peuvent notamment porter sur :
  - la détection des anomalies et la surveillance des comportements des agents;
  - l'évaluation de la sécurité et les simulations d'attaque de type « red teaming »;
  - l'exploitation de la confiance dans les interactions entre humains et agents;
  - les risques systémiques (risque de concentration, infrastructures critiques, perte d'intégrité de l'écosystème informationnel);
  - les normes et garanties pour réduire les failles de cybersécurité.

- **Outils de sécurité adaptés aux modèles à poids ouverts :** Concevoir des outils et des cadres destinés à réduire les obstacles au déploiement sûr et sécurisé des modèles à poids ouverts grâce à des mesures de protection solides et à un contrôle rigoureux des risques. Les projets peuvent notamment porter sur :
  - les protocoles de mesure et d'évaluation;
  - les tests d'évaluation des performances en matière de sécurité;
  - les normes internationales et les exigences des politiques.

Admissibilité et modalités de financement

Volet A — Projets canadiens

Les propositions peuvent être présentées par un maximum de deux chercheuses ou chercheurs principaux (CP) rattachés à une faculté d'une université canadienne.

Dans le cadre de ce volet, un montant de 80 000 $ CA sera remis à la ou au CP pour couvrir le salaire et les avantages sociaux d'une chercheuse ou d'un chercheur postdoctoral pendant un an. Une enveloppe supplémentaire de 20 000 $ sera attribuée à chaque équipe pour couvrir les avantages et les coûts directs de la recherche (p. ex., les frais informatiques et les déplacements nécessaires à la présentation des travaux dans des colloques).

Volets B — Projets en partenariat

Les propositions doivent être présentées par au moins deux chercheuses ou chercheurs principaux (CP) en vue d'une collaboration franco-canadienne ou germano-canadienne.

L'une ou l'un des CP doit être rattaché à une faculté d'une université canadienne.

La ou le deuxième CP doit satisfaire à l'un des critères suivants :

- **Inria** : faire partie d'une équipe de recherche de l'Inria en France;
- **CISPA** : faire partie du corps enseignant du CISPA en Allemagne.

Le financement versé aux CP couvrira le salaire et les avantages sociaux d'une chercheuse ou d'un chercheur postdoctoral pendant un maximum de deux ans. Le montant accordé pour une chercheuse ou un chercheur postdoctoral établi en Allemagne ou en France suivra le barème habituel de l'organisme partenaire, jusqu'à concurrence de 150 000 $ CA par année.

Présentation des demandes

Calendrier

Les propositions de projets Catalyseur doivent être déposées sur le portail SurveyMonkey du CIFAR entre le **23 novembre 2026 et le 4 janvier 2027, à 23 h 59 (heure AoE, soit le dernier fuseau horaire de la planète).** N'oubliez pas de cliquer sur le bouton d'envoi pour finaliser votre demande.

Pour toute question ou demande de renseignements, écrivez-nous à ai@cifar.ca.

- **Début de la période de dépôt des demandes :** le 23 novembre 2026
- **Date limite de dépôt des demandes :** le 4 janvier 2027
- **Communication prévue des décisions :** février 2027
- **Attribution du financement :** au plus tard le 31 mars 2027
- **Démarrage des projets :** entre mars et octobre 2027

le portail SurveyMonkey du CIFAR

Exigences liées au projet

Veuillez soumettre un document PDF en français ou en anglais contenant les renseignements suivants :

- Titre du projet;
- Nom, affiliation(s) et adresse courriel de la, du ou des CP soumettant le projet;
- **Description du projet (maximum de 7 pages, sans les références) :**
  - Objectifs, démarche méthodologique et théorique, résultats escomptés, calendrier et principales étapes du projet;
  - Originalité, importance et retombées sociétales possibles du projet (p. ex., orientation des politiques publiques, réduction des préjudices, renforcement de la confiance du public, inclusion de groupes dignes d'équité);
  - Ressources informatiques nécessaires et moyens prévus pour y accéder, s'il y a lieu;
  - Concordance du projet avec les priorités de cet appel de propositions et du Programme de recherche de l'ICSIA au CIFAR.
- Présentation de l'équipe : quelle expertise cette équipe apporte-t-elle au projet et en quoi cette expertise est-elle essentielle à son avancement (1/2 page max.)?
- Date de début envisagée du projet (entre mars et octobre 2027)
- Nom, affiliation(s) et adresse courriel des collaboratrices et collaborateurs confirmés (s'il y a lieu);
- CV à jour de toutes les parties prenantes connues (autrices ou auteurs de la demande, collaboratrices ou collaborateurs et étudiantes ou étudiants).

Critères de sélection

Le conseil de recherches de l'ICSIA et des spécialistes externes évalueront les propositions selon les critères suivants :

- Originalité et importance de la proposition : 35 %
- Retombées sociétales attendues du projet : 25 %
- Excellence du dossier de recherche des autrices et auteurs de la demande : 15 %
- Faisabilité du projet (calendrier, ressources disponibles, expertise de l'équipe) : 15 %
- Concordance avec les axes prioritaires de l'appel de propositions : 10 %

Utilisation de l'IA générative

L'utilisation de l'IA générative est permise aux fins de la préparation des demandes. Les personnes candidates doivent toutefois s'assurer que l'ensemble du contenu généré est exact, complet et pertinent, et en assumer l'entière responsabilité. L'autrice ou l'auteur de la demande demeure entièrement responsable de la qualité et de l'intégrité du contenu.

Conformément à sa politique, le CIFAR applique les lignes directrices des organismes fédéraux de financement de la recherche en ce qui concerne l'utilisation de l'IA générative dans les demandes de financement.

Exigences de présentation de l'information

- Les personnes retenues doivent remettre au CIFAR un rapport sur les principales conclusions et retombées de leurs travaux dans les 45 jours suivant la fin de la première année et la conclusion du projet.
- Les personnes retenues devront assister à la rencontre annuelle du Programme de recherche de l'ICSIA à l'automne 2027 et pourraient être invitées à y présenter leurs travaux. Les frais de déplacement seront pris en charge.