# Process Overview for CBRF-BRIF

- TIPS' dedicated research security team reviews the Risk Assessment Form as part of the administrative process, prior to merit review. This process includes **ensuring completeness of the form** as well as an **administrative risk validation** using open-source intelligence (OSINT) methods.
- Where necessary, TIPS requests **national security risk assessment and advice.** These are cases where:
  - the nature of the proposed research is deemed sensitive (Annex A) and
  - the private sector partner organization were identified from open-source information to be:
    - associated with, or originating from, countries/organizations under sanctions, and/or
    - criminal or ethical concerns are raised.

# Process Overview for CBRF-BRIF

- When requested, Canada's national security departments and agencies assess the risks associated with the research partnership, consider the proposed mitigations, and provide advice to TIPS and CFI.
- If a research partnership proposal is assessed to present an unacceptable risk to Canada's national security and/or where risks cannot be appropriately mitigated, the application will be removed from the competition.

# New Attestation requirement

- New research security attestation requirement further to ministers statement of February 14, 2023.
- Implementation date to be confirmed, however it is expected that it will apply to CBRF-BRIF.
- Institutions will be required to indicate whether, if funded, the grant will support research in a listed sensitive research area and will be required to certify, by means of attestation forms, that no researcher involved in the activities supported by the grant is affiliated with or receiving funding or in-kind support from any listed university, research institute, or laboratory.
- More information will be shared as soon as it is available.

# Updated version

- Innovation, Science and Economic Development (ISED) Canada, in consultation with the federal granting agencies, CFI and the national security departments and agencies, has updated the Risk Assessment Form (RAF).

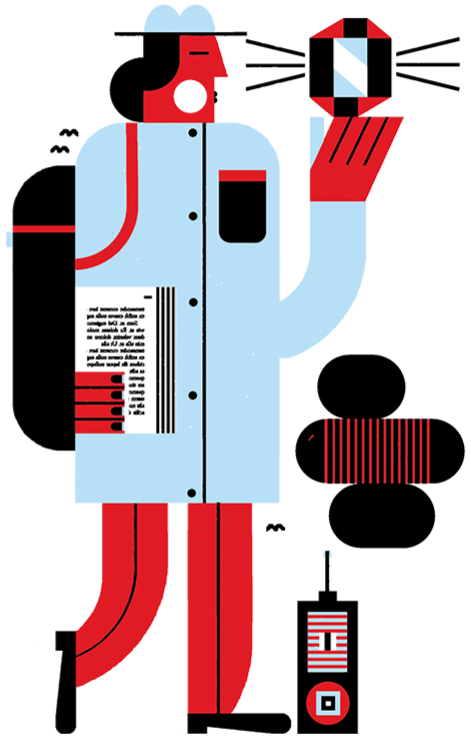
- On March 24, 2023, the updated RAF was posted on the Safeguarding Your Research portal.

- Changes to the RAF were informed by feedback received from the research community, including by a survey on the implementation of the National Security Guidelines for Research Partnerships (Guidelines) conducted by the U15 Group of Canadian Research Universities and Universities Canada in Summer 2022.

# Overview

- **Questions —**Additional information is included to help applicants complete each question and to reduce the need to refer to separate documents or pieces of legislation.
- **Risk Assessment Process —** The “Overview of the Process” and “Process flow chart” is presented on a new **Risk Assessment Review Process** page of the Safeguarding Your Research portal.
- **Annex A (Sensitive Research Areas) —** To more easily hyperlink to sections of Annex A within the Risk Assessment Form, the list of sensitive and dual-use research areas and sensitive personal data in the Annex are integrated into two distinct tables.
- **Risk Mitigation Plan Information —** Helpful information to assist in developing a Risk Mitigation Plan is presented on a new **Mitigating Your Research Security Risks** page on the Safeguarding Your Research portal.

# Best Practices



# When completing the risk assessment form:

- ✓ Researchers and institutions should use the tools and resources on the Safeguarding Your Research portal for information on how to identify and mitigate risks to security in research partnerships.

- ✓ Ensure to read the form in its entirety and consult any external resources mentioned in the form to ensure your responses are as accurate as possible.

- ✓ Have open discussions with your partner organization(s) to identify potential or perceived risks.

- ✓ Conduct **open source intelligence due diligence** to identify any potential or perceived risks related to your partner organization(s).

# Open Source Intelligence (OSINT) Due Diligence

- Conducting OSINT due diligence will help you answer the questions on “Know Your Partner”.
- A new **Guide on Conducting Open Source Due Diligence** is now available on the Safeguarding Your Research Portal.
- The goal is to verify that your research partners are who they say they are and to ensure their relationships and motivations are clear.
- OSINT due diligence helps you find some risk indicators like:
  - Structures or relationships that may compromise your partner’s autonomy
  - Indications of connections to foreign governments, militaries or security services on sensitive research areas
  - Information that shows your partner operates in countries known to steal intellectual property from researchers
  - Any information that suggests lack of transparency

# Risk Identification and Risk Mitigation Plan

- Risk identification and a risk mitigation plan are required whenever there is a **“yes” or “unsure”** in **section 1 (Know Your Research) and/or section 2 (Know Your Partner).**
- Risk mitigation measures are required even if there are no risks with the partner, but the research could still be a target. Use your best judgement and show due diligence when developing a mitigation plan that addresses the potential risks you have identified.
- It’s not sufficient to refer to existing or upcoming policies and practices within the institution, you must describe what this policy or practice entails and how it will be applied to mitigate the identified risks.
- Excluding any individual from participating in the proposed research project on the basis of their citizenship or country of residence is not an acceptable risk mitigation measure.

Consult the **Mitigating Your Research Security Risks** on the Safeguarding Your Research portal for detailed guidance on how to best prepare the Risk Mitigation Plan section of the form.

# Risk Mitigation Plan

Mitigation measures should be tailored to the research project and commensurate with the risks identified while considering open science principles. Mitigation plans can cover areas, such as, but not limited to:

- **Describing any other relevant review processes for which the project has been subject to**
  *e.g., Has the project been reviewed by any internal committees to determine how the data should be specifically safeguarded?*
- **Raising research security awareness and building capacity across your research team**
  *e.g., Have the institution committed to providing training to members of the research team around Research Security related topics?*
- **Ensuring that partner organization(s)' objectives align with the objectives of the partnership**
  *e.g., Has the institution discussed with your partner what they hope to gain from the partnership?*
- **Ensuring sound cybersecurity and data management practices**
  *e.g., Are there device management protocols for professional and personal international travel for-this project?*
- **Agreement on the intended use of research findings**
  *e.g., How will Intellectual Property be handled with the research team, collaborators, and partner organization(s)?*

# FRENCH VERSION FOLLOWS

# Vue d'ensemble du processus pour FRBC- FIRSB

- Une équipe dédiée du SPIIE examine le formulaire d'évaluation des risques dans le cadre du processus administratif, avant l'examen du mérite. Ce processus consiste à **assurer que le formulaire est complet** et à effectuer une **validation administrative des risques** à l'aide de méthodes de renseignement de source ouverte.
- Au besoin, le SPIIE demande une **évaluation des risques et des avis en matière de sécurité nationale.** Ce sont les cas où:
  - la nature de la recherche proposée est considérée comme sensible (annexe A) et
  - les organisations partenaires du secteur privé ont été identifiées, à partir d'informations provenant de sources ouvertes, comme étant:
    - associés à ou originaires de pays/organisations soumis à des sanctions, et/ou
    - des préoccupations d'ordre criminel ou éthique.

# Vue d'ensemble du processus pour FRBC- FIRSB

- Au besoin, les ministères et organismes responsables de la sécurité nationale du Canada évaluent les risques associés au partenariat de recherche, examinent les mesures d'atténuation proposées et fournissent des conseils au SPIIE et à la FCI.
- Si une proposition de partenariat de recherche est jugée comme présentant un risque inacceptable pour la sécurité nationale du Canada et/ou si les risques ne peuvent être atténués de manière appropriée, la demande sera retirée du concours.

# Nouvelle exigence en matière d’attestation

- Nouvelle exigence en matière d'attestation de sécurité de la recherche suite à la déclaration des ministres du 14 février 2023.
- La date de mise en œuvre reste à confirmer, mais il est prévu qu'elle s'appliquera pour FRBC- FIRSB.
- Les établissement devront indiquer si, en cas de financement, la subvention soutiendra la recherche dans un domaine de recherche sensible figurant sur la liste et devront certifier, au moyen de formulaires d'attestation, qu'aucun chercheur participant aux activités soutenues par la subvention n'est affilié à une université, un institut de recherche ou un laboratoire figurant sur la liste, ni ne reçoit de financement ou de soutien en nature.
- De plus amples informations seront communiquées dès qu'elles seront disponibles.

# Mise à jour

- Innovation, Science et Développement économique (ISDE) Canada, en consultation avec les organismes subventionnaires fédéraux, la FCI et les ministères et organismes chargés de la sécurité nationale, a mis à jour le formulaire d'évaluation des risques.

- Le 24 mars 2023, le formulaire mis à jour a été publié sur le portail Protégez votre recherche, remplaçant la version précédente.

- Les changements apportés au formulaire ont été guidés par les commentaires reçus de la communauté des chercheurs, notamment par une enquête sur la mise en œuvre des lignes directrices sur la sécurité nationale pour les partenariats de recherche (lignes directrices) menée par le groupe U15 des universités de recherche canadiennes et Universités Canada au cours de l'été 2022.

# Changements principaux

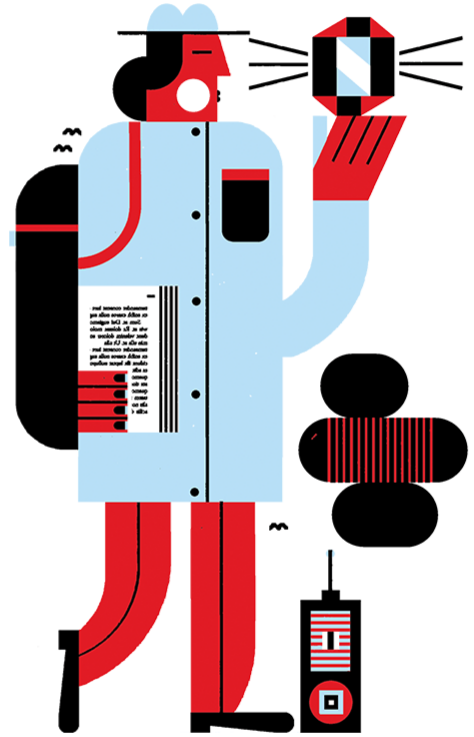
- **Questions —** Toutes les questions ont été simplifiées et reformulées pour plus de clarté. Des informations supplémentaires ont été ajoutées pour aider les candidats à répondre à chaque question et pour réduire la nécessité de se référer à des documents ou à des textes législatifs distincts.

- **Processus d'évaluation des risques —** « L’aperçu du processus » et « le schéma de processus » qui se trouvaient en annexe du formulaire original ont été supprimés. Ces informations ont été mises à jour et sont désormais présentées sur une nouvelle page **Processus d’examen de l’évaluation des risques** du portail Protégez votre recherche.

- **Annexe A (domaines de recherche sensible ou à double usage) —** Pour faciliter la création de liens hypertextes vers les sections de l'annexe A dans le formulaire d'évaluation des risques, la liste des domaines de recherche sensibles et à double usage et des données personnelles sensibles de l'annexe a été intégrée dans deux tableaux distincts.

- **Information sur le plan d’atténuation des risques —** Les informations sur l'atténuation des risques ont été retirées du nouveau formulaire et sont désormais présentées sur une nouvelle page intitulée **Atténuez les risques liés à la sécurité de la recherche** sur le portail Protéger votre recherche.

# Meilleures pratiques



# Lorsque vous remplissez le formulaire d'évaluation des risques:

- ✓ Les chercheurs et les établissements devraient utiliser les outils et les ressources du portail **Protégez votre recherche** pour obtenir des informations sur la manière d'identifier et d'atténuer les risques pour la sécurité dans les partenariats de recherche.

- ✓ Veillez à lire le formulaire dans son intégralité et à consulter toute ressource externe mentionnée dans le formulaire afin de vous assurer que vos réponses sont aussi précises que possible.

- ✓ Avoir des discussions ouvertes avec votre ou vos organismes partenaires pour identifier les risques potentiels ou perçus

- ✓ **Faire preuve de diligence raisonnable en matière de sources ouvertes** pour identifier tout risque potentiel ou perçu lié à votre ou vos organisations partenaires.

# Faire preuve de diligence raisonnable en matière de sources ouvertes

- Effectuer de telles recherches vous aidera à répondre aux questions de la rubrique « À propos de votre partenaire ».
- Un nouveau **Guide sur la conduite d'une recherche de diligence raisonnable en matière de sources ouvertes** est désormais disponible sur le portail Protégez votre recherche.
- L'objectif est de vérifier que vos partenaires de recherche sont bien ceux qu'ils affirment être et de s'assurer que leurs liens et leurs motivations sont clairs.
- Information de sources ouvertes vous aideront à trouver certains indicateurs de risque tels que :
  - Des structures organisationnelles ou des liens qui peuvent limiter ou compromettre l'indépendance ou l'autonomie de votre partenaire.
  - Des indices que votre partenaire est associé à un gouvernement étranger dans des domaines de recherche sensibles.
  - Des indices qui montrent que votre partenaire opère dans des pays connus pour voler la propriété intellectuelle des chercheurs.
  - Toute information qui ne correspond pas à ce que votre partenaire vous a déclaré

# L’identification des risques et le Plan atténuation des risques

- L'identification des risques et un plan d'atténuation des risques sont requis chaque fois qu'il y a un **« oui »** ou un **« pas sur »** à la **section 1 (Connaissez votre recherche) et/ou à la section 2 (Connaissez votre organisme partenaire).**
- Des mesures d'atténuation des risques sont nécessaires même s'il n'y a pas de risques avec le partenaire, mais que la recherche peut toujours être une cible. Faites preuve de discernement et de diligence lors de l'élaboration d'un plan d'atténuation des risques potentiels que vous avez identifiés.
- Il ne suffit pas de faire référence aux politiques et pratiques existantes ou à venir au sein de l'institution, vous devez décrire ce que cette politique ou cette pratique implique et comment elle sera appliquée pour atténuer les risques identifiés.
- L'exclusion d'une personne de la participation au projet de recherche proposé en raison de sa citoyenneté ou de son pays de résidence n'est pas une mesure d'atténuation des risques acceptable.

Consultez la page **Atténuez les risques liés à la sécurité de la recherche** sur le portail Protégez votre recherche pour obtenir des conseils détaillés sur la meilleure façon de préparer la section Plan d'atténuation des risques du formulaire.

# Plan d'atténuation des risques

Les mesures d'atténuation doivent être adaptées au projet de recherche et proportionnées aux risques identifiés tout en tenant compte des principes de la science ouverte. Les plans d'atténuation peuvent couvrir des domaines tels que, mais sans s'y limiter :

- **Décrire toute autre procédure d'examen pertinente à laquelle le projet a été soumis.**
  *Par exemple, le projet a-t-il été examiné par des comités internes afin de déterminer comment les données doivent être spécifiquement protégées ?*
- **Sensibilisation à la sécurité de la recherche et renforcement des capacités au sein de votre équipe de recherche**
  *Par exemple, l'établissement s'est-il engagé à fournir une formation aux membres de l'équipe de recherche sur des sujets liés à la sécurité de la recherche ?*
- **Veiller à ce que les objectifs de l'organisation ou des organisations partenaire(s) s'alignent sur les objectifs du partenariat**
  *Par exemple, est-ce que l'établissement a discuté avec votre partenaire de ce qu'il espère retirer du partenariat ?*
- **Assurer des pratiques saines en matière de cybersécurité et de gestion des données**
  *Par exemple, existe-t-il des protocoles de gestion des appareils pour les voyages internationaux professionnels et personnels effectués dans le cadre de ce projet ?*
- **Accord sur l'utilisation prévue des résultats de la recherche**
  *Par exemple, comment la propriété intellectuelle sera-t-elle gérée avec l'équipe de recherche, les collaborateurs et le(s) organisation(s) partenaire(s) ?*