NSERC and Canada's Research Security Policies

Presented by NSERC's Research Security Team

Canada's approach to research security

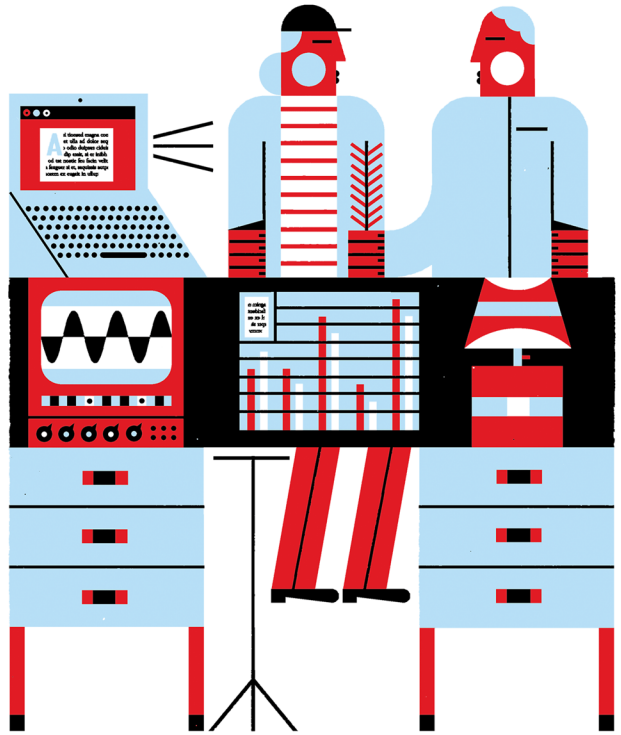
Research security refers to the actions that safeguard the integrity of research domestically and internationally, with a particular emphasis on protecting against threats to national and economic security. This includes actions that safeguard against the theft and misappropriation of research, as well as the unauthorized transfer of ideas, research outcomes, and intellectual property.

Canada's approach to research security has been informed by ongoing dialogue and collaboration with Canada's research community and it aligns with international best practices such as the G7 Common Values and Principles of Research Security and Integrity.

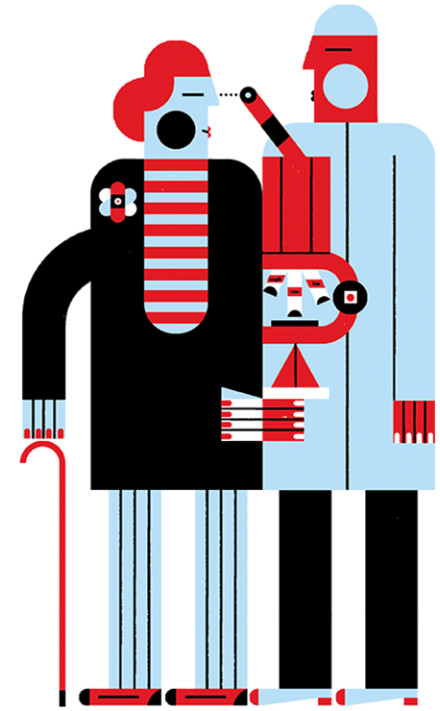
The Government of Canada, granting agencies, and research community have a **shared responsibility** to:

- Protect the integrity of our research ecosystem and to safeguard it from activities that undermine its principles of openness, transparency, merit, academic freedom, and reciprocity; and,
- Ensure that research security measures (new and existing) do not lead to discrimination against or profiling of any member of the community.

Table of contents



Policy on Sensitive Technology Research and Affiliations of Concern



Overview of the STRAC Policy

- On February 14, 2023, the federal government announced its intent to adopt an enhanced posture regarding Canada's research security.
- The policy was developed through **collaboration** between federal departments and agencies and in **consultation** with the research community through the Government of Canada-Universities Working Group.
- On January 16, 2023, the Government of Canada announced the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy).
- The policy operates using two lists that **must be used in conjunction** — a list of Sensitive Technology Research Areas (STRA) and a list of Named Research Organizations (NRO).
- The granting agencies and the CFI will implement the policy in harmonized manner, starting with funding opportunities launching as of **May 1st, 2024**.

Core Statement of the STRAC Policy

Grant applications submitted by a university or affiliated research institution to the federal granting agencies and the CFI involving research that advances a sensitive technology research area will not be funded if any of the researchers involved in activities supported by the grant are affiliated with, or in receipt of funding or in-kind support, from a university, research institute or laboratory connected to military, national defence or state security entities that could pose a risk to Canada's national security.

Core Statement of the STRAC Policy

Grant applications submitted by a university or affiliated research institution to the federal granting agencies and the CFI involving research that advances a sensitive technology research area will not be funded if any of the researchers involved in activities supported by the grant are affiliated with, or in receipt of funding or in-kind support, from a university, research institute or laboratory connected to military, national defence or state security entities that could pose a risk to Canada's national security.

Two lists that operate in conjunction

Sensitive Technology Research Areas (STRA)

- Composed of 11 high-level technology categories at various stages of development.
- The sub-categories indicate the specific **sensitive technology research areas** of concern.
- The specific concern is the **advancement** of a technology during the course of the research.
- Research that will use, but not advance, an existing technology is not within the scope of this policy.

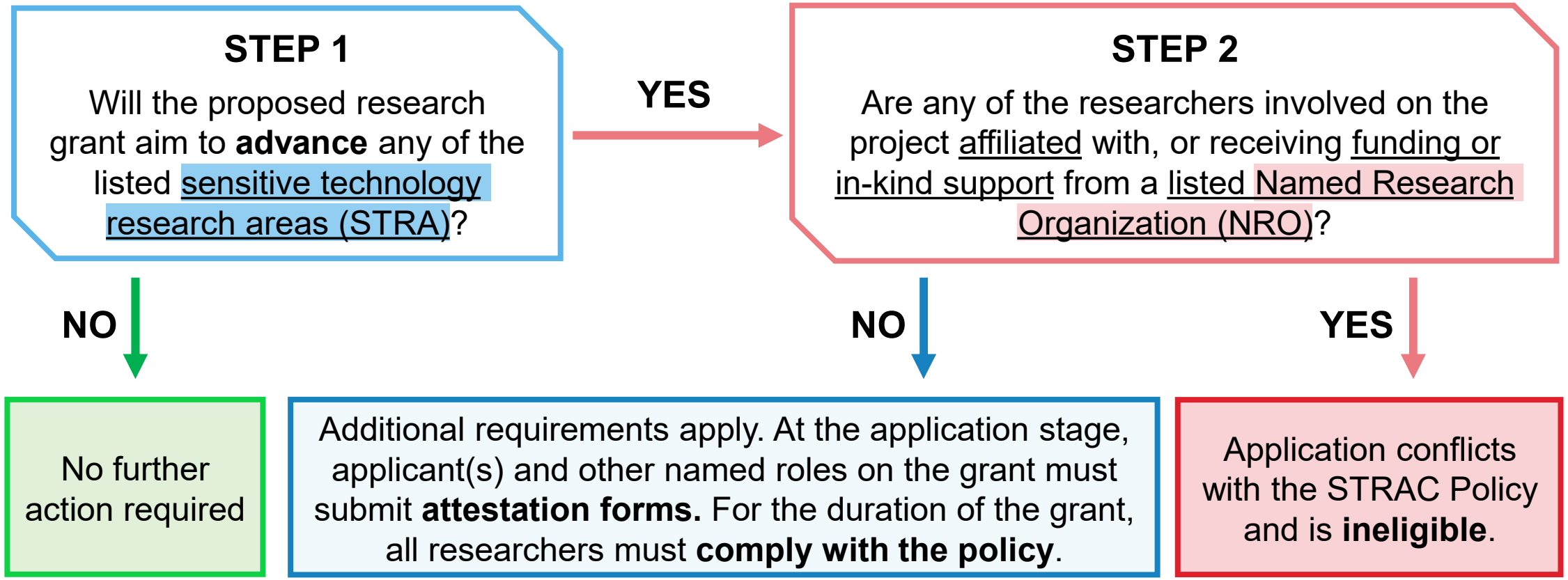
Both lists will be updated regularly to address evolving threats to Canada's national security.

Named Research Organizations (NRO)

- Composed of **103 research organizations and institutions** that pose the highest risk to Canada's national security due to their direct or indirect connections with military, national defence, and state security entities.
- The STRAC policy concerns the institutions listed on the NRO list.
- At all times, researchers are encouraged to apply due diligence practices to mitigate risks that may be associated with any collaboration or partnership in a sensitive technology research area – even if an institution is not included in the current list.

Compliance with the STRAC Policy

When considering applying for a grant funding opportunity that is in-scope for the STRAC Policy, applicants will follow a **two-step process** to determine what requirements apply:



Next Steps

STRAC Policy is announced

Funding organizations publish **guidance, procedures**, and **forms**

STRAC requirements implemented into relevant grant funding opportunities as they launch

January-February

March-May

January

February-March

May ⟶

Implementation and targeted consultation by the funding organizations

Information sessions and **webinars** in both official languages

National Security Guidelines for Research Partnerships

Overview of the NSGRP

- In July 2021, the Government of Canada introduced the National Security Guidelines for Research Partnerships (NSGRP) to integrate national security considerations into the development, evaluation, and funding of research partnerships. They were designed in consultation with the Government of Canada – Universities Working Group.
- The NSGRP process applies to certain research partnership funding programs, where applicants are required to complete a **Risk Assessment Form** to identify risks and mitigation measures associated with their **research** and their **partner organization**.
- The NSGRP are **country- and company-agnostic**, recognizing that security risks evolve and can come from anywhere in the world, and follow a set of guiding principles:

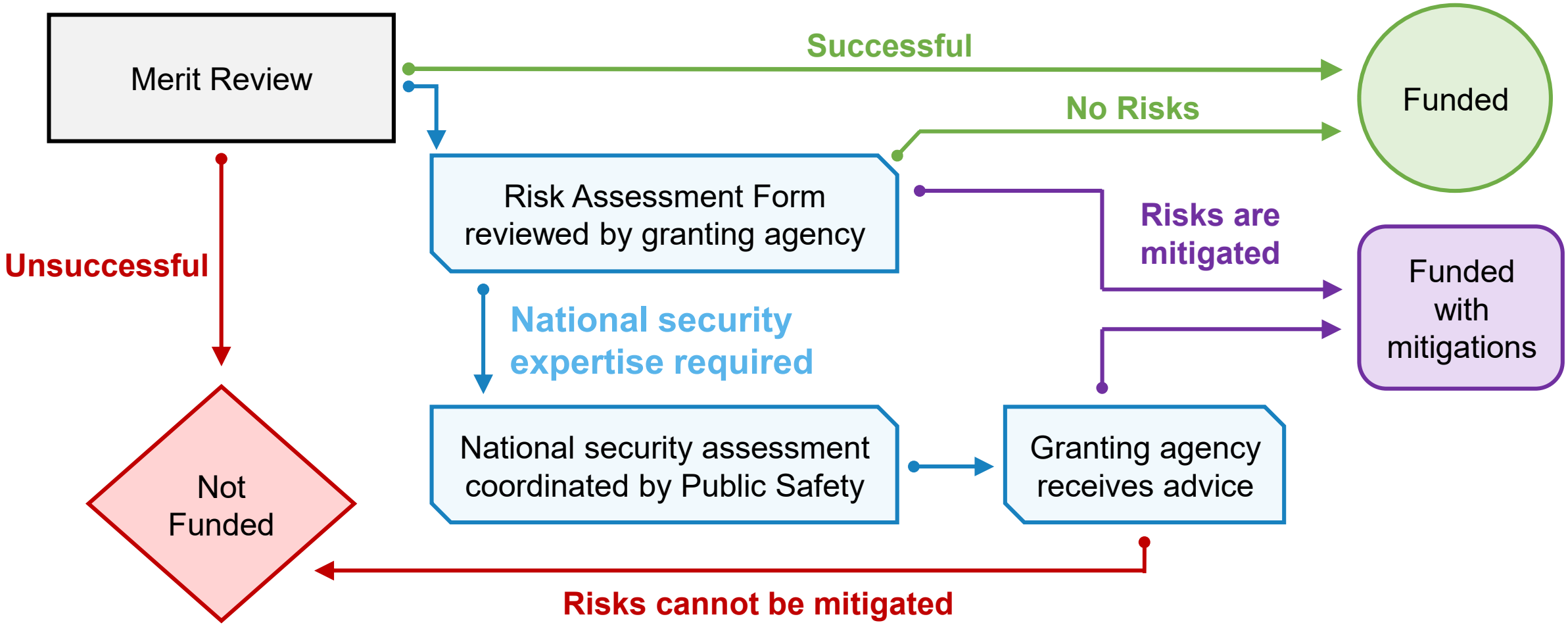
✓ Academic Freedom
✓ Institutional Autonomy
✓ Freedom of Expression
✓ Transparency
✓ Integrity
✓ Collaboration
✓ Equity, Diversity, and Inclusion
✓ Research in the Public Interest

Implementation of the NSGRP Process

- To date, the NSGRP process applies to NSERC's Alliance program and to the second stage of the TIPS-CFI joint Canada Biomedical Research Fund and Biosciences Research Infrastructure Fund competition for applications with private sector partner organizations.
- The risks addressed by the NSGRP relate to the **research** and the **partner organization**:

Know Your Research	Know Your Partner
If your research: ✓ May be dual-use ✓ Advances a sensitive research area like critical minerals or has sensitive datasets; and/or ✓ Could advance a foreign state's military or defence capabilities and negatively impact Canada Then, **your research may be at risk**	If your private sector research partner may: ✓ Transfer knowledge to a foreign government, military or other actor that could harm Canada's national security interests; and/or ✓ Lack the autonomy and independence that underpins an open and transparent research ecosystem Then, **your partner may pose a risk**

NSGRP Risk Assessment Review Process



Impact of the NSGRP on NSERC's Alliance grants program

NSERC analyzed data from the implementation in Alliance (July 2021 – July 2023). As of July 31, 2023:

Status of applications received that required a Risk Assessment Form (RAF)	
6.5 %	Applications **rejected or returned** due to research security administrative review
2.5%	Applications **still under evaluation**
61.6%	Applications **funded** by NSERC without requiring national security risk assessment
27.1%	Applications **not funded** due to program administrative or merit review
3.1%	Applications **referred to** national security agencies for risk assessment and advice

74% of rejected or returned applications were successfully resubmitted

*40% posed **no risk***
*60% had **appropriate mitigations** in place*

Out of 62 applications
*2 were **withdrawn***
*22 were **funded***
*38 were **not funded***

- **Success rates for applications to the Alliance program have not changed,** including for applicants who self-identified as a visible minority.
- NSERC's administrative risk validation **adds on average 1-2 days to the processing time of ~97% of Alliance applications.**
- **Additional processing time is required for the ~3.1% of cases** where applications required advice from the national security departments and agencies; clear service standards for this process are in development.

Updates to the NSGRP

March 2023

- Lessons learned and community feedback led to an updated Risk Assessment Form with increased clarity and usability, and with greater focus on EDI and non-discrimination.
- New guidance on conducting open-source due diligence and on mitigating research security risks added to the Safeguarding Your Research portal, including a new self-paced web-course.

January 2024

- First annual NSGRP Progress Report (2021-2023) is published.
- Sensitive Research Areas list (Annex A – List 1) is replaced by the List of Sensitive Technology Research Areas to align with the STRAC Policy.
- The implementation of the NSGRP is ongoing. Next phases will be **gradual, risk-based,** and **limited** to funding opportunities that support partnerships. Further details will be announced in funding opportunity literature.

Risk Assessment Form Overview & Best Practices

Overview

- The Risk Assessment Form (RAF) is a tool to identify and assess potential risks that research partnerships may pose to Canada's national security as outlined in the National Security Guidelines for Research Partnerships and to develop effective mitigation measures.

- A completed RAF **must** be included with **any Alliance Grants application involving one or more private sector partner organizations, industrial associations, or producer groups**. When submitting an Alliance Grant application, the RAF must be uploaded in the "Other Documents" section of NSERC's Online System.

Section 1: Know Your Research

- The purpose of this section is to gather key information about the research. This information will be used to assess whether the **nature and/or usability of your research project** could attract the interest of **foreign governments, militaries, their proxies, and other organizations** who may seek to exploit research partnerships to access research information, research knowledge, and the resulting intellectual property and technology to facilitate unauthorized knowledge transfer.

- This section references multiple resources including:

• The Critical Minerals List • The National Strategy for Critical Infrastructure	• The Export Control List • Annex A of the National Security Guidelines for Research Partnerships

It is essential to consult these resources when completing this section to ensure your responses are as accurate as possible.

Section 2: Know Your Partner Organization

- The purpose of this section is to assess whether your partner organization(s) could pose a national security risk by using the research knowledge, technology and intellectual property resulting from your research project.

- Answer the questions in this section to the best of your ability by using information that is already available to you, your institution, or your partner organization(s), or that could be reasonably accessed through open sources via **Open Source Intelligence Due Diligence**.

- When answering these questions, you must consider and include information not only about your partner organization(s) but also their relevant affiliates such as any affiliated **parent organizations, subsidiaries,** and **joint ventures in Canada and abroad**.

Section 2: Know Your Partner Organization: question 2.4

- Question 2.4 asks "***Are there any indications that as a result of this research project, your partner organization(s) will or could have access to your research institution's Canadian facilities, networks, or assets on campus, including infrastructure that houses sensitive data?*** "
  - This questions is asking if your partner organization will gain access to your institution's infrastructure or data unrelated to this project ***because*** of this specific partnership.
  - **This question does not ask if your partner organization already has legitimate access to infrastructure or data at your institution due to other partnerships or projects.**

Open Source Intelligence (OSINT) Due Diligence

- Conducting OSINT due diligence will help you answer the questions in **Section 2: Know Your Partner**.
- A **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

Section 3: Risk Identification

- The purpose of this section is to collect information on any risk factors that you have identified in **Section 1: Know Your Research** and **Section 2: Know Your Partner Organization**. To support the risk assessment process, your response must provide information on the source and nature of the risks.

Section 4: Risk Mitigation Plan

- The purpose of this section is to demonstrate you've identified the appropriate mitigation measures to reduce the likelihood of an identified security risk materializing, and/or to lessen the impact in case the identified risk materializes.

Section 3: Risk Identification and **Section 4: Risk Mitigation Plan** **must** be completed if **any** questions in **Section 1: Know Your Research** and **Section 2: Know Your Partner Organization** are answered **"Yes"** or **"Unsure".**

Risk Identification and Risk Mitigation Plan

- 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 your 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 you committed to providing training to members of your research team around Research Security related topics?
- **Ensuring that your partner organization(s)' objectives align with the objectives of the partnership**
  e.g., Have you 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 travels occurring during this project?
- **Agreement on the intended use of research findings**
  e.g., How will Intellectual Property be handled with your research team, your collaborators, and your partner organization(s)?

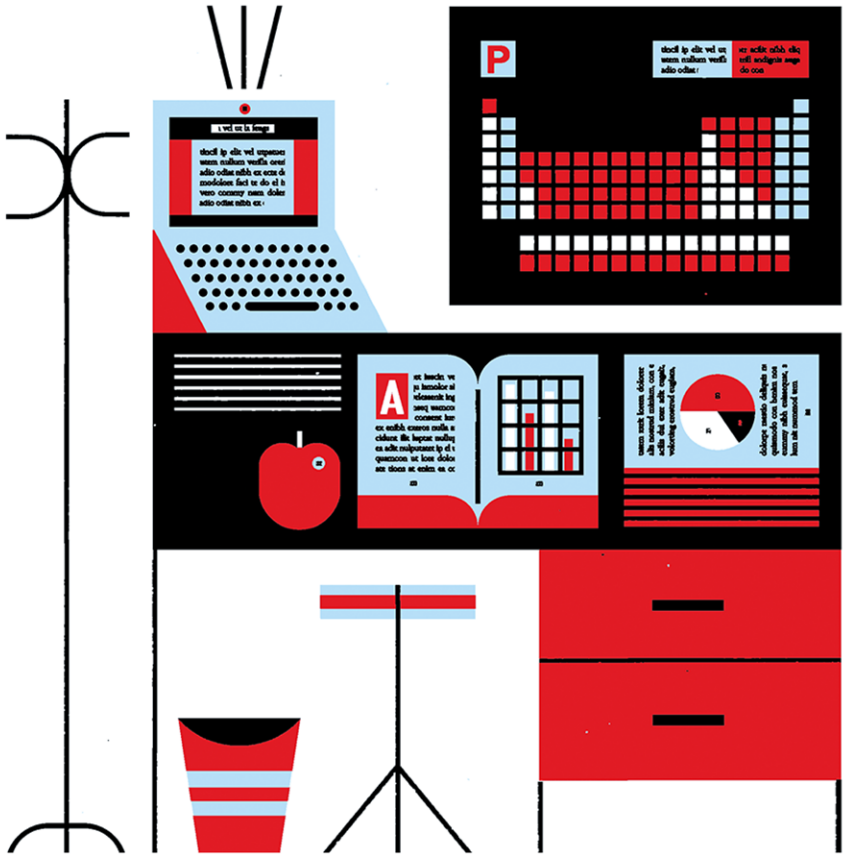
Section 5: Additional Requirements

- This section includes the following two statements that the applicant must agree to, on behalf of all co-applicants (if applicable), by submitting the RAF:

  - The applicant(s) have not accepted and will not accept any offer of funding that is conditional upon the mirroring of their academic laboratory in, or the transfer of their academic laboratory to, a foreign country
  - The source of funding and the value of the research project to the partner organization(s) has been communicated by the partner organization(s) to the applicant(s)

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).



Questions?

Research Security

Research Partnerships, NSERC

researchsecurity@nserc-crsng.gc.ca

Connect with us

@nserc_crsng

facebook.com/nserccanada