Government of Canada Gouvernement du Canada

Canada

Implementation of the Policy on Sensitive Technology Research & Affiliations of Concern (STRAC)

Table of Contents

1. Background on Research Security
2. The Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)
    - Overview of the policy
    - Implementation by the granting agencies
    - Compliance mechanisms
3. STRAC and the National Security Guidelines for Research Partnerships (NSGRP)
4. Resources

Background on research security

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.

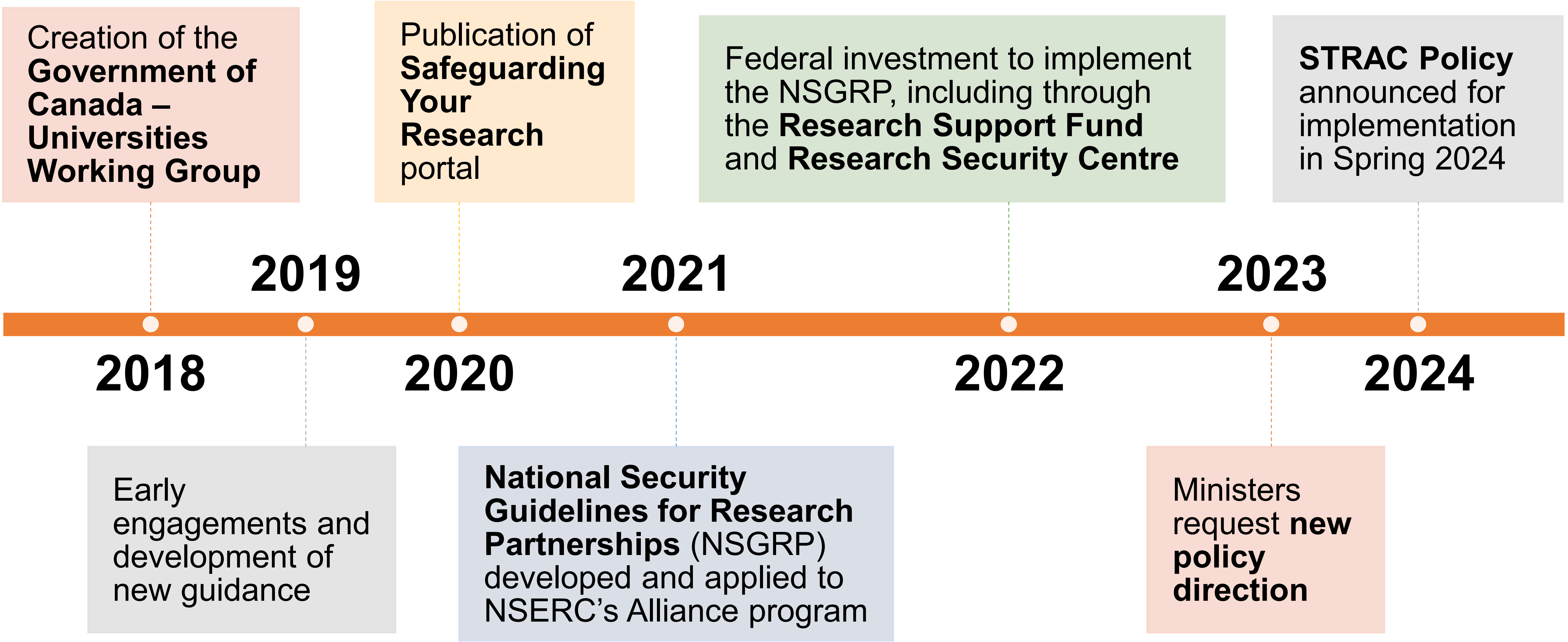
The Government of Canada, granting agencies, and research community have a **shared responsibility** to:

- 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.

Background on research security

Timeline of Canadian Research Security Policy



2018

Creation of the **Government of Canada – Universities Working Group**

2019

Early engagements and development of new guidance

2020

Publication of **Safeguarding Your Research** portal

2021

National Security Guidelines for Research Partnerships (NSGRP) developed and applied to NSERC's Alliance program

2022

Federal investment to implement the NSGRP, including through the **Research Support Fund** and **Research Security Centre**

2023

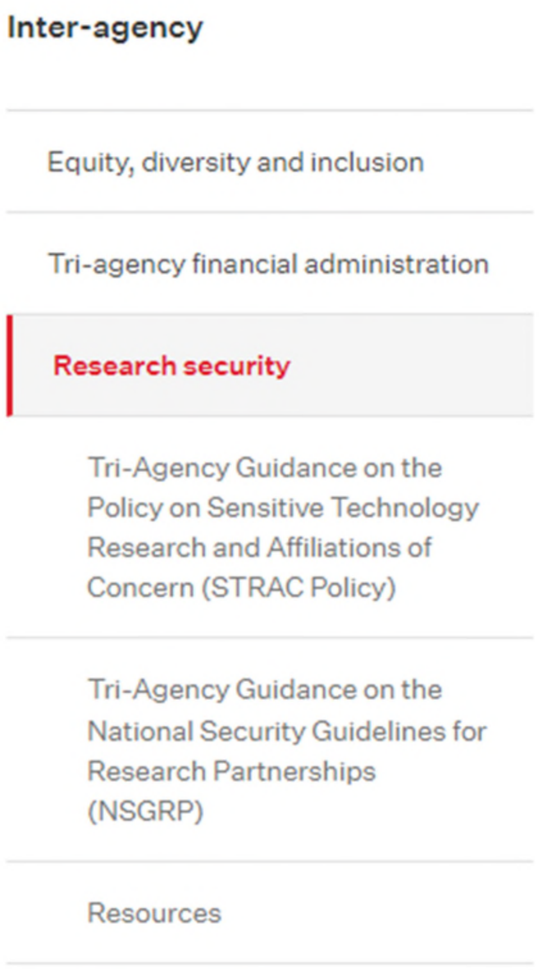
Ministers request **new policy direction**

2024

STRAC Policy announced for implementation in Spring 2024

Background on Research Security

New Tri-Agency Guidance on Research Security



Inter-agency

Equity, diversity and inclusion

Tri-agency financial administration

Research security

Tri-Agency Guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)

Tri-Agency Guidance on the National Security Guidelines for Research Partnerships (NSGRP)

Resources

- This new webpage provides guidance regarding the implementation of research security measures by the federal granting agencies (NSERC, SSHRC, and CIHR).
- We encourage all members of the research community to familiarize themselves with this guidance, and as well as the linked policies, guidelines, and resources.

On this page:

- General guidance and guiding principles
- Tri-Agency Guidance on the STRAC Policy
- Tri-Agency Guidance on the National Security Guidelines for Research Partnerships
- Resources

Policy on Sensitive Technology Research and Affiliations of Concern (STRAC):

- Overview of the policy

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, 2024, 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).
- Modalities of the granting agencies' implementation of this policy were published on March 28, 2024, through the Tri-Agency Guidance on the STRAC Policy.

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.

The Policy on Sensitive Technology Research and Affiliations of Concern (STRAC)

Two lists that operate in conjunction

Sensitive Technology Research Areas (STRA)

- Composed of 11 high-level technology categories.
- 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.

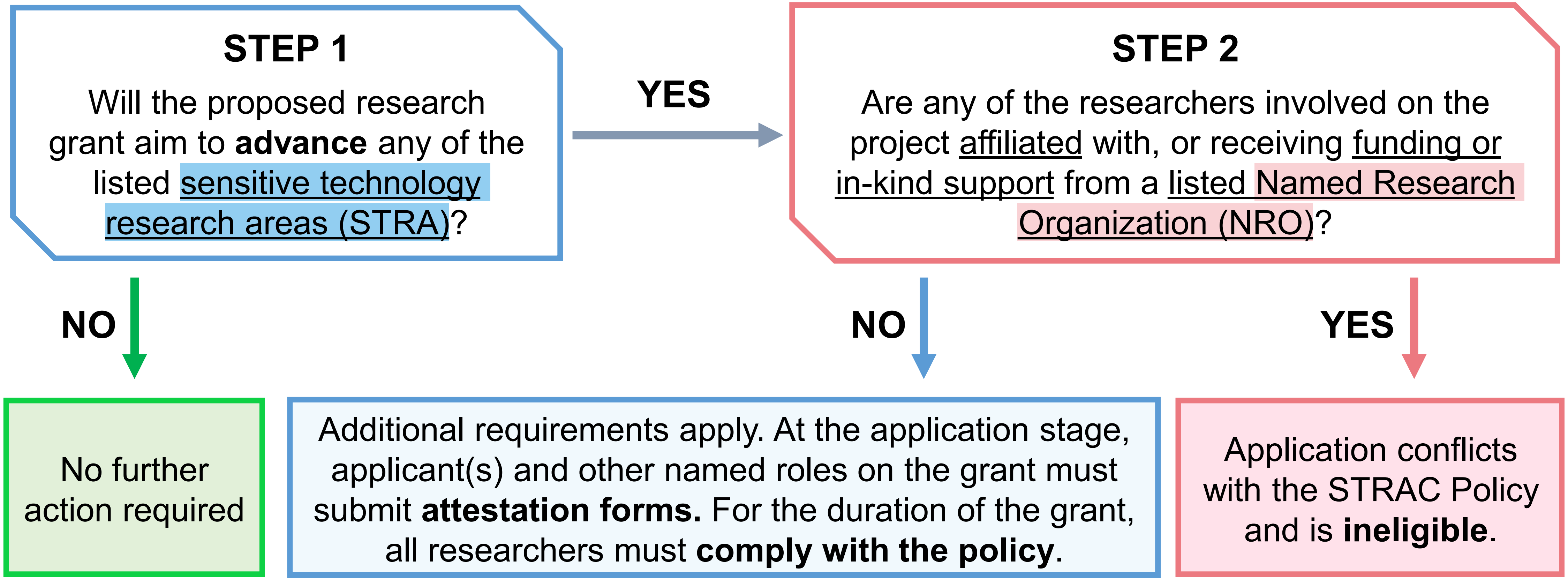
Both lists will be updated regularly to address evolving threats to Canada's national security.

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.

Two-Step process to comply with the 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:



STEP 1

Will the proposed research grant aim to **advance** any of the listed sensitive technology research areas (STRA)?

YES

STEP 2

Are any of the researchers involved on the project affiliated with, or receiving funding or in-kind support from a listed Named Research Organization (NRO)?

NO

No further action required

NO

Additional requirements apply. At the application stage, applicant(s) and other named roles on the grant must submit **attestation forms.** For the duration of the grant, all researchers must **comply with the policy**.

YES

Application conflicts with the STRAC Policy and is **ineligible**.

Step 1 – When should a proposed research grant be identified as “aiming to advance a STRA”?

If the research supported during the course of the grant aims to support the **generation or discovery of knowledge that contributes to progress in the development of a technology described in the list of Sensitive Technology Research Areas.**

- The list is composed of high-level technology categories, where the **sub-categories** indicate the sensitive technology research areas of concern.
- Research not covered by the **sub-categories** of the list, or that will merely use but not advance an existing technology, is not considered sensitive within the scope of this policy.

Step 2 – Who must comply with the STRAC Policy

If the grant is identified by the applicant as **aiming to advance a STRA:**

- **Application Stage:** Researchers with named roles in the grant application must submit attestation forms to certify their own compliance with the policy.
  - Named roles at NSERC and SSHRC include, where applicable: the applicant, co-applicants, collaborators, project directors, co-directors, or other equivalent roles.
  - Named roles at CIHR include the Nominated Principal Applicant, Principal Applicants, Co-Applicants, Principal Knowledge Users, and Knowledge Users. Unlike NSERC and SSHRC, this does not include Collaborators.
  - Attestations are personal and cannot be provided on behalf of others.
- **Duration of the Grant:** All researchers – including all HQP and collaborators – involved in research activities supported by the grant must comply with the policy for the duration of the grant.

STRAC Policy:

- Implementation by the granting agencies

Tri-Agency Guidance on the STRAC Policy

- The granting agencies are implementing the STRAC Policy in a harmonized manner and on a forward basis, starting with funding opportunities launching as of **May 1st, 2024**.
- The Tri-Agency Guidance on the STRAC Policy describes the granting agencies' harmonized approach, as well as agency-specific information, including:
  - New **procedures** and **forms**;
  - Responsibilities of **researchers** and **institutions**;
  - The **list of funding opportunities** in scope of the policy; and
  - A list of **Frequently Asked Questions**.
- This Tri-Agency guidance was informed by a consultation with Canadian universities, conducted in coordination with Universities Canada and the U15 in February 2024.
- This approach is aligned with the Canada Foundation for Innovation, which published dedicated guidance to outline its implementation of research security measures.

New procedures and forms

Application stage

- Funding opportunity literature will clearly **indicate** whether the STRAC policy applies
- **New modules** added to the grant management system
- **Attestation Form** for Research Aiming to Advance Sensitive Technology Research Areas

Compliance mechanisms throughout the duration of the grant

- New **terms and conditions** of the grant
- Attestation and STRA **validation processes**
- Alignment with processes under the Tri-Agency Framework: Responsible Conduct of Research (RCR Framework)

New modules in the grant management systems

- When preparing a research grant application for a funding opportunity that is applying the STRAC Policy, **two new modules** will appear in the grant management systems.
- Both modules are only accessible to the **primary applicant**.

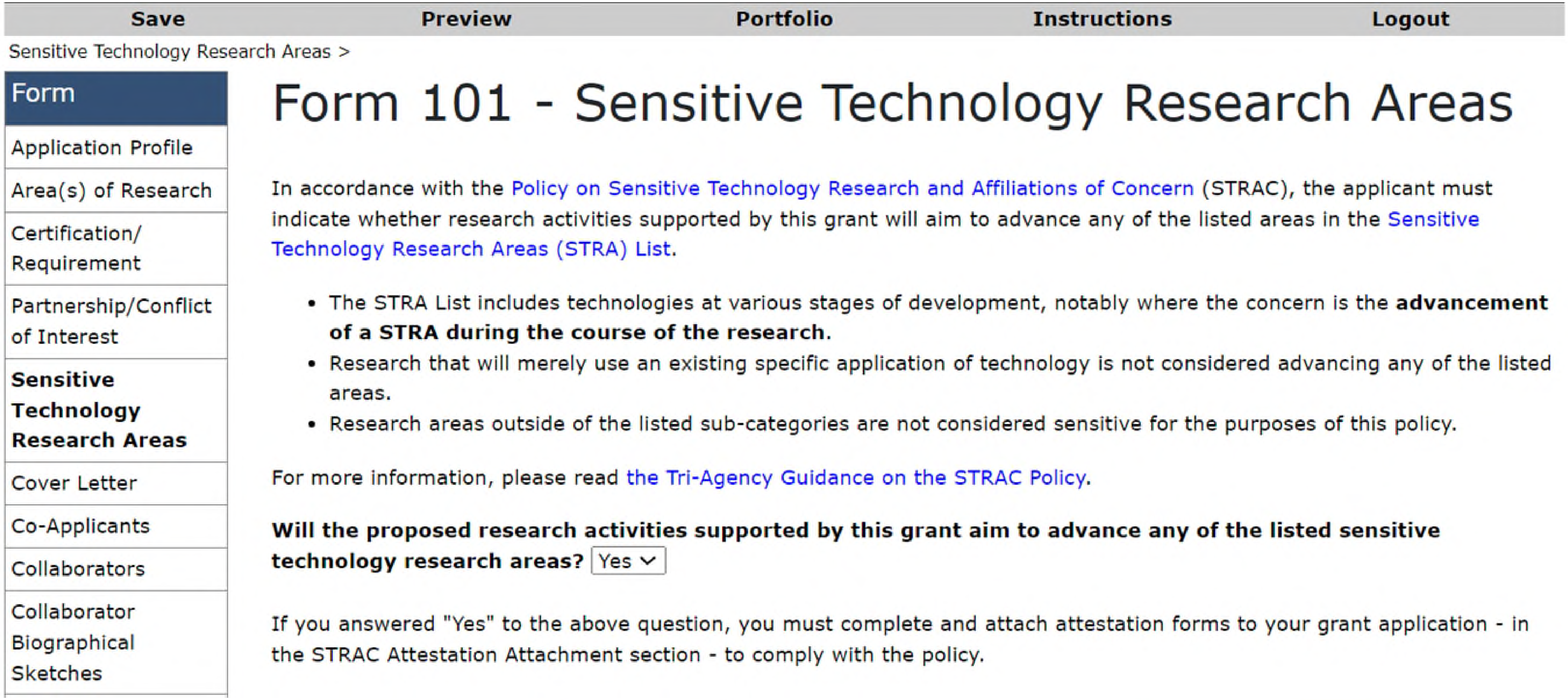
Sensitive Technology Research Area module (mandatory)

- The primary applicant will be asked whether their proposed research will **aim to advance a STRA**.
- They must answer the question with a **Yes / No response**, on behalf of the research team.

Attestation Form module (mandatory if applicant responded "Yes" to the STRA module)

- Module includes a URL pointing toward the **attestation form** template.
- Researchers with named roles must each complete an attestation form.
- The primary applicant will collect all individual attestation forms, save them as a single PDF file, and upload it to the grant management system.

Example module on Sensitive Technology Research Areas


Save
Preview
Portfolio
Instructions
Logout
Sensitive Technology Research Areas >
Form
Application Profile
Area(s) of Research
Certification/ Requirement
Partnership/Conflict of Interest
Sensitive Technology Research Areas
Cover Letter
Co-Applicants
Collaborators
Collaborator Biographical Sketches

Form 101 - Sensitive Technology Research Areas

In accordance with the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC), the applicant must indicate whether research activities supported by this grant will aim to advance any of the listed areas in the Sensitive Technology Research Areas (STRA) List.

- The STRA List includes technologies at various stages of development, notably where the concern is the **advancement of a STRA during the course of the research.**
- Research that will merely use an existing specific application of technology is not considered advancing any of the listed areas.
- Research areas outside of the listed sub-categories are not considered sensitive for the purposes of this policy.

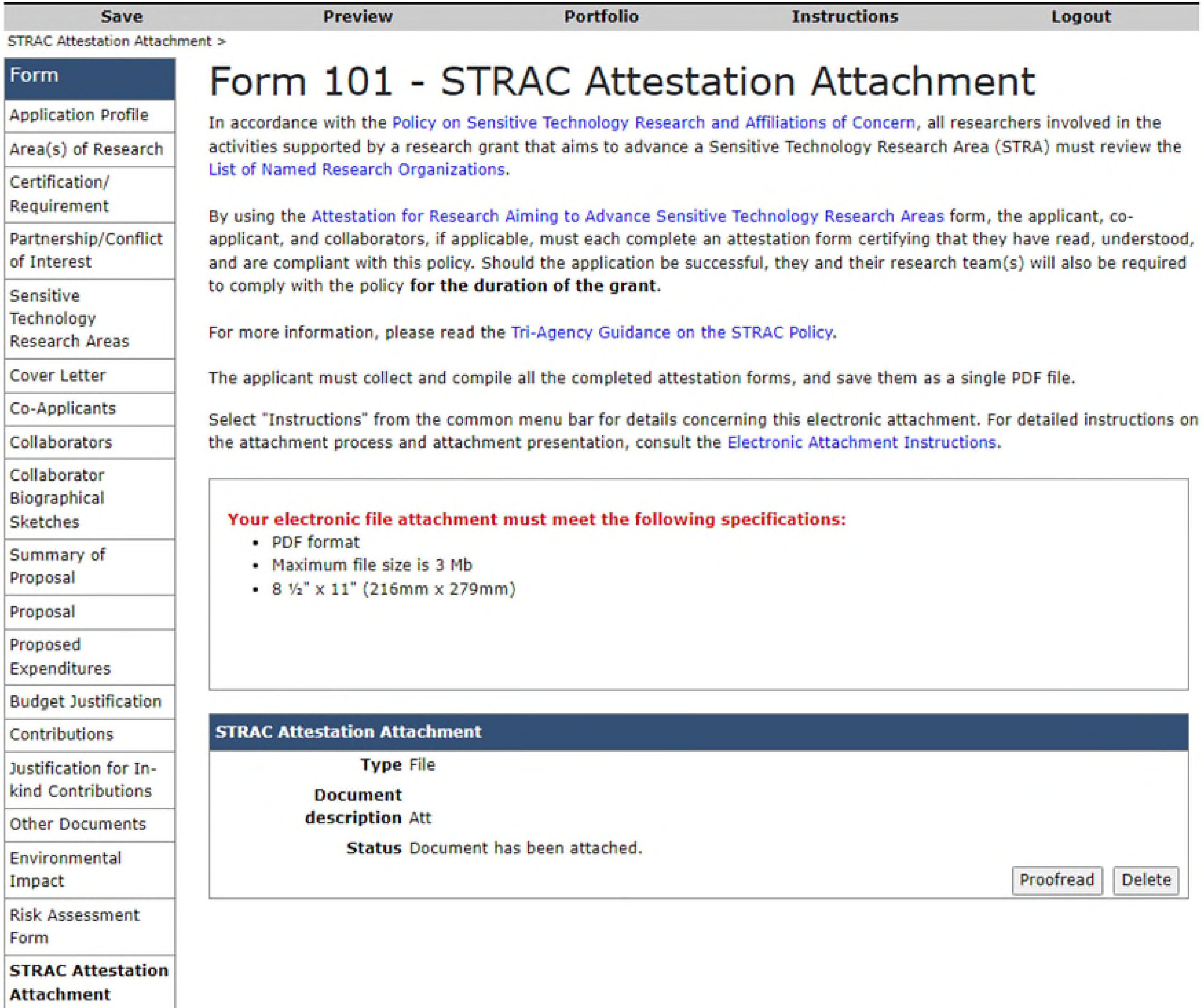
For more information, please read the Tri-Agency Guidance on the STRAC Policy.

Will the proposed research activities supported by this grant aim to advance any of the listed sensitive technology research areas? Yes

If you answered "Yes" to the above question, you must complete and attach attestation forms to your grant application - in the STRAC Attestation Attachment section - to comply with the policy.

The Policy on Sensitive Technology Research and Affiliations of Concern (STRAC)

Example module on the STRAC Attestation Attachment



Form 101 - STRAC Attestation Attachment

In accordance with the Policy on Sensitive Technology Research and Affiliations of Concern, all researchers involved in the activities supported by a research grant that aims to advance a Sensitive Technology Research Area (STRA) must review the List of Named Research Organizations.

By using the Attestation for Research Aiming to Advance Sensitive Technology Research Areas form, the applicant, co-applicant, and collaborators, if applicable, must each complete an attestation form certifying that they have read, understood, and are compliant with this policy. Should the application be successful, they and their research team(s) will also be required to comply with the policy **for the duration of the grant**.

For more information, please read the Tri-Agency Guidance on the STRAC Policy.

The applicant must collect and compile all the completed attestation forms, and save them as a single PDF file.

Select "Instructions" from the common menu bar for details concerning this electronic attachment. For detailed instructions on the attachment process and attachment presentation, consult the Electronic Attachment Instructions.

Your electronic file attachment must meet the following specifications:

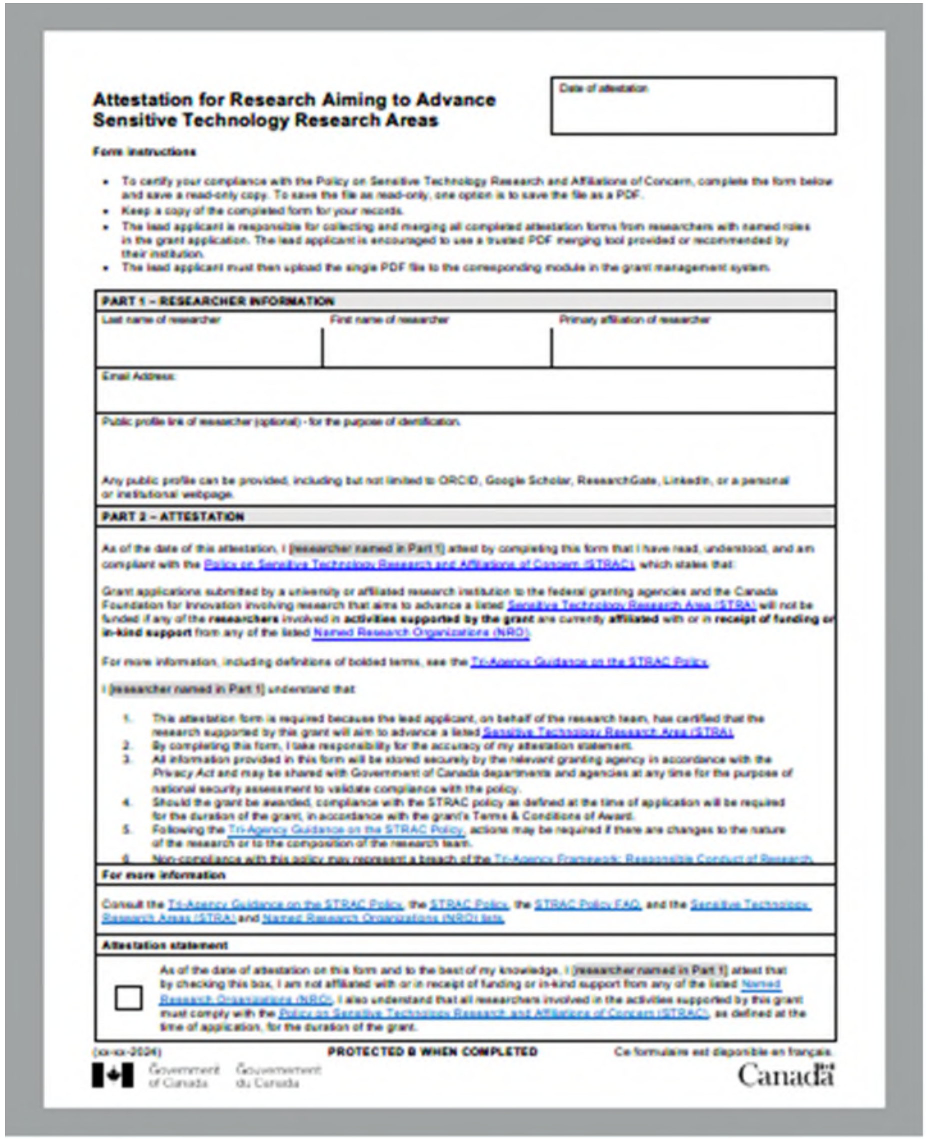
- PDF format
- Maximum file size is 3 Mb
- 8 ½" x 11" (216mm x 279mm)

STRAC Attestation Attachment

Type	File
Document description	Att
Status	Document has been attached.

Attestation form template

- The attestation form is available through the Tri-Agency Guidance on the STRAC Policy.
- The same **simple, one-page form-fillable PDF** is used by all three granting agencies.
- A new form is required from each researcher in a named role, for each grant application that is identified as *aiming to advance a STRA*.
- Attestations forms will be considered following the versions of the STRA and NRO lists that were publicly available on the date indicated.



Attestation for Research Aiming to Advance Sensitive Technology Research Areas

Date of attestation

Form instructions

- To certify your compliance with the Policy on Sensitive Technology Research and Affiliations of Concern, complete the form below and save a read-only copy. To save the file as read-only, one option is to save the file as a PDF.
- Keep a copy of the completed form for your records.
- The lead applicant is responsible for collecting and merging all completed attestation forms from researchers with named roles in the grant application. The lead applicant is encouraged to use a trusted PDF merging tool provided or recommended by their institution.
- The lead applicant must then upload the single PDF file to the corresponding module in the grant management system.

PART 1 – RESEARCHER INFORMATION

Last name of researcher

First name of researcher

Primary affiliation of researcher

Email Address

Public profile link of researcher (optional) - for the purpose of identification.

Any public profile can be provided, including but not limited to ORCID, Google Scholar, ResearchGate, LinkedIn, or a personal or institutional webpage.

PART 2 – ATTESTATION

As of the date of this attestation, I [researcher named in Part 1] attest by completing this form that I have read, understood, and am compliant with the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC), which states that:

Grant applications submitted by a university or affiliated research institution to the federal granting agencies and the Canada Foundation for Innovation involving research that aims to advance a listed Sensitive Technology Research Area (STRA) will not be funded if any of the **researchers** involved in **activities supported by the grant** are currently **affiliated** with or in **receipt of funding or in-kind support** from any of the listed Named Research Organizations (NRO).

For more information, including definitions of bolded terms, see the Tri-Agency Guidance on the STRAC Policy.

I [researcher named in Part 1] understand that:

1. This attestation form is required because the lead applicant, on behalf of the research team, has certified that the research supported by this grant will aim to advance a listed Sensitive Technology Research Area (STRA).
2. By completing this form, I take responsibility for the accuracy of my attestation statement.
3. All information provided in this form will be stored securely by the relevant granting agency in accordance with the *Privacy Act* and may be shared with Government of Canada departments and agencies at any time for the purpose of national security assessment to validate compliance with the policy.
4. Should the grant be awarded, compliance with the STRAC policy as defined at the time of application will be required for the duration of the grant, in accordance with the grant's Terms & Conditions of Award.
5. Following the Tri-Agency Guidance on the STRAC Policy, actions may be required if there are changes to the nature of the research or to the composition of the research team.
6. Non-compliance with this policy may represent a breach of the Tri-Agency Framework: Responsible Conduct of Research.

For more information

Consult the Tri-Agency Guidance on the STRAC Policy, the STRAC Policy, the STRAC Policy FAQ, and the Sensitive Technology Research Areas (STRA) and Named Research Organizations (NRO) lists.

Attestation statement

□ As of the date of attestation on this form and to the best of my knowledge, I [researcher named in Part 1] attest that by checking this box, I am not affiliated with or in receipt of funding or in-kind support from any of the listed Named Research Organizations (NRO). I also understand that all researchers involved in the activities supported by this grant must comply with the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC), as defined at the time of application, for the duration of the grant.

(xx-xx-2024) **PROTECTED B WHEN COMPLETED** Ce formulaire est disponible en français.

Government of Canada Gouvernement du Canada Canada

Responsibilities of Researchers

Following the **updated terms and conditions of award** for funding opportunities where STRAC applies, grant recipients must inform the corresponding granting agency and their institutional officials

- If the grant was originally identified as **not aiming to advance a STRA**, and the nature of the research changes such that it is now **aiming to advance a STRA**.
  - Grant recipients cannot proceed with these new research activities until the granting agency's approval has been obtained. New requirements will apply under the STRAC Policy.
  - If the resulting change causes a conflict with the policy due to the involvement of a NRO, the granting agency will work with the relevant institution(s) to address the issue and to determine the best route forward to minimize impacts, on the research, the grant, and associated research personnel.
- If the composition of the **researchers in named roles** changes, in which case existing processes for grant amendment under the Tri-Agency Guide on Financial Administration should be followed.
  - Attestation forms from new researchers in a named role would be required. They cannot begin work on activities supported by the grant until the granting agency's approval has been obtained.

Responsibilities of Researchers

Following the **updated terms and conditions of award** for funding opportunities where STRAC applies:

- All research team members involved in the activities funded by a grant that was identified as **aiming to advance a STRA** – including all collaborators and highly qualified personnel (HQP) – are **individually responsible** for ensuring that they do not hold an active affiliation or receive funding or in-kind support from any of the listed Named Research Organizations, following the versions of the lists that were publicly available on the date that the grant application was submitted.
  - This requirement applies for the duration of their involvement in the activities supported by the grant, regardless of whether an attestation form was required at the time of application.
- Grant recipients should ensure that all prospective research team members are aware of their individual responsibilities with regards to compliance with the STRAC Policy.

Responsibilities of Institutions

Institutions should support their researchers in being compliant with the STRAC Policy, using the resources offered and promoted by the Government of Canada. Research Grant Officers should (with support from their institutional research security office, where available):

- Ensure researchers **understand their individual responsibilities** under the STRAC Policy, during the grant application process and following the terms and conditions of the grant.
- Perform a **completeness check** to ensure that all required attestation forms have been provided with the application, if the applicant has identified that the grant will aim to advance a listed Sensitive Technology Research Area.
  - Research Grant Officers are **not** expected to validate the accuracy of attestation forms.
- Institutions may support their grantees in following best practices, including to conduct open-source due diligence when seeking to recruit new prospective research team members and/or to develop new collaborations and partnerships.

STRAC Policy:

- Compliance mechanisms

Validation of STRAs

- The granting agencies will conduct **periodic validations** on a **randomized subset of funded grants** to ensure that applicants have appropriately identified whether their grant would *aim to advance a STRA*.

- To minimize bias, sample selection will be based solely on **unique alphanumerical identifiers** associated with each application. The funding organizations will ensure that the random sample is representative of all relevant funding opportunities.

- In cases where the validation process uncovers information suggesting that a grant application should have been identified as *aiming to advance a STRA*, the agency will inform the applicant and may request the submission of attestation forms.

The Policy on Sensitive Technology Research and Affiliations of Concern (STRAC)

Validation of Attestation Forms

Validation will occur through one of two streams, with support from Public Safety Canada:

1. For most funding opportunities and programs, attestation forms will be validated periodically, on a **randomized subset of funded grants**. This validation process will be conducted ***post* funding decision** and therefore will not impact the service standards of funding opportunities.
2. For funding opportunities where the National Security Guidelines for Research Partnerships also apply, validation of attestation forms will be completed **in parallel** for any application that is referred to the national security departments and agencies for their assessment and advice following the Risk Assessment Review Process.

If information is uncovered suggesting that a researcher may be in breach of the policy, the granting agency will work with the relevant institution(s) to address the issue and to determine the best route forward to minimize impacts, on the research, the grant, and associated research personnel.

Further action may be taken to address the issue, up to an including an allegation of breach of the Tri-Agency Framework: Responsible Conduct of Research.

Interaction of the STRAC Policy and the Tri-Agency Framework: Responsible Conduct of Research

- The STRAC policy is within scope of Article 2.4 of the Tri-Agency Framework: Responsible Conduct of Research regarding **Agency Requirements for Certain Types of Research.**
- Failure to comply with the STRAC policy when conducting research activities related to a grant identified as **aiming to advance a STRA** may invoke an allegation of **Breach of Agency Policies or Requirements for Certain Types of Research** per Article 3.1.4.
- Provision of an inaccurate **Attestation form** as part of an Agency application may invoke an allegation of **misrepresentation in an Agency Application or Related Document** per Article 3.1.2.
- Should there be an allegation of breach by a researcher, this will be communicated to the SRCR. Following the established RCR process, the researcher’s institution will be responsible for conducting an inquiry and, where necessary, an investigation.

RCR Framework: Recourse

- Following Article 4.3.4, investigation processes are conducted by a committee appointed by the researcher's institution. The respondent is provided an opportunity to be heard as part of the investigation and may appeal if a breach of policy is confirmed.
- Recourse for breaches of the RCR Framework varies by severity, intentionality, and impact of the breach, as per Article 6.1.3 of the Framework. Recourse may include, but is not limited to:
  - A letter of awareness;
  - Withholding installments of and/or termination of the funding;
  - A requirement to reimburse funds; and
  - Ineligibility to hold/apply for federal funding for a defined period of time or permanently.
- In exercising the appropriate recourse, the corresponding granting agency will give consideration to affected research personnel including students, post-doctoral fellows and research support staff.
- Decisions on RCR cases are not normally communicated beyond the three Agencies, except to the institution where the respondent is employed, if that was the investigating institution.

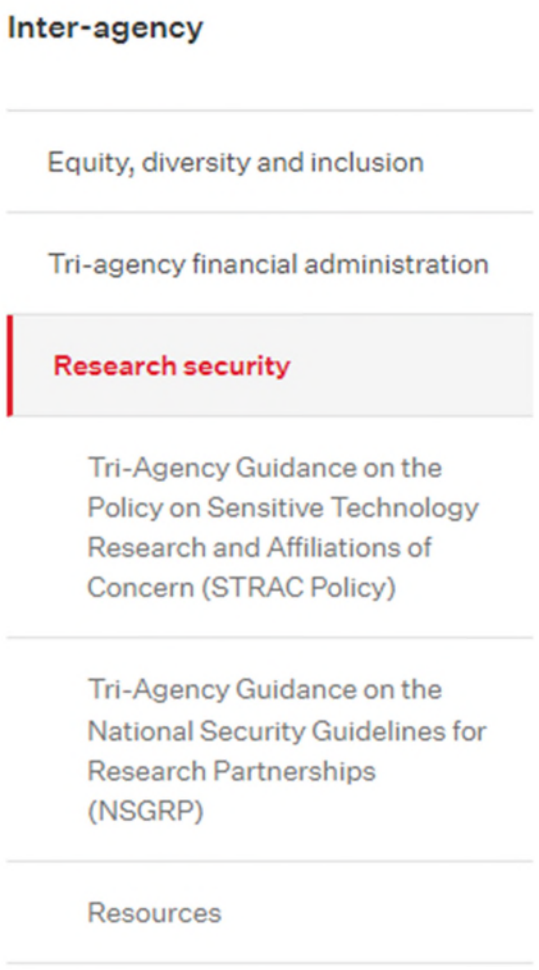
STRAC and the National Security Guidelines for Research Partnerships (NSGRP)

NSGRP	VS.	STRAC Policy
Risks related to the **research project** and the **private sector partner organization(s)**	**Risks Addressed**	**Sensitive technology research** performed with **research organizations and institutions** that pose the highest risk to Canada’s national security
A **Risk Assessment Process** that supports the identification, analysis and mitigation of risks as part of the development, evaluation, and funding of research partnerships.	**Mechanism**	A **policy requirement** that applies to research grants that **aim to advance a sensitive technology research area (STRA)**
Applicable to **selected** federal research partnership funding programs	**Applicability**	Applicable to **all** relevant federal research grant funding opportunities that fund university-based research
Applicants seeking grant funding for research with a private sector partner complete a **Risk Assessment Form**	**Requirements at the application stage**	Researchers with named roles on the grant application must complete an **Attestation Form**
Grant recipients must implement any **risk mitigation measures** identified in their Risk Assessment Form and in their Notice of Decision.	**Requirements for the duration of the grant**	Researchers involved in activities supported by the grant cannot hold a **current affiliation**, or be **in receipt of funding or in-kind support** from a **named research organization (NRO)**

Resources

Resources

New **Tri-Agency Guidance on Research Security**



Inter-agency

Equity, diversity and inclusion

Tri-agency financial administration

Research security

Tri-Agency Guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)

Tri-Agency Guidance on the National Security Guidelines for Research Partnerships (NSGRP)

Resources

- This new webpage provides guidance regarding the implementation of research security measures by the federal granting agencies (NSERC, SSHRC, and CIHR).
- We encourage all members of the research community to familiarize themselves with this guidance, and as well as the linked policies, guidelines, and resources.

On this page:

- General guidance and guiding principles
- Tri-Agency Guidance on the STRAC Policy
- Tri-Agency Guidance on the National Security Guidelines for Research Partnerships
- Resources

Resources

Recommended resources:

Canada’s Research Security Centre, hosted by Public Safety Canada:

- Inbox: researchsecurity-securiteenrecherche@ps-sp.gc.ca
- Connect with a Regional Advisor
- Safeguarding Science - Workshop Information

Safeguarding Your Research Portal:

- Guidance for Research Organizations and Funders on Developing a Research Security Plan (science.gc.ca)
- Guidance on Conducting Open Source Due Diligence (science.gc.ca)
- Research Security Training Courses (science.gc.ca)
- Mitigating Your Research Security Risks (science.gc.ca)

Other resources offered by Universities Canada and the U15:

- Safeguarding Research in Canada: A Guide for University Policies and Practices

Contact us:

NSERC:
researchsecurity@nserc-crsng.gc.ca

CIHR:
support-soutien@cihr-irsc.gc.ca

SSHRC:
researchsecurity-securiterecherche@sshrc-crsh.gc.ca