Government of Canada | Gouvernement du Canada

Canada

Policy on Sensitive Technology Research and Affiliations of Concern

This publication is available online at https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/policy-sensitive-technology-research-and-affiliations-concern.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at https://ised-isde.canada.ca/site/publications or contact:

ISED Citizen Services Centre

Innovation, Science and Economic Development Canada

C.D. Howe Building

235 Queen Street

Ottawa, ON K1A 0H5

Canada

Telephone (toll-free in Canada): 1-800-328-6189

Telephone (international): 613-954-5031

TTY (for hearing impaired): 1-866-694-8389

Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Email: ISED@canada.ca

Reproduction Authorization

Cat. No. Iu37-43/2023E-PDF

ISBN 978-0-660-67911-2

Aussi offert en français sous le titre Aperçu et orientations : Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes.

Table of Contents

New Policy on Sensitive Technology Research and Affiliations of Concern

Canada's world-class research ecosystem is defined by excellence and its open and collaborative nature. This openness can make it a target for foreign influence that increases the potential for research and development efforts to be misappropriated to the detriment of national security. For example, the illicit transfer of knowledge - especially in transformational research areas such as AI, quantum computing, and genetic engineering that could have dual-use applications for military and surveillance purposes - poses major challenges to Canada and its allies.

The federal government has been active in supporting researchers and institutions to protect Canada's research, providing advice and tools through the Safeguarding Your Research portal, and implementing national security considerations into the development, evaluation, and funding of research partnerships through the National Security Guidelines for Research Partnerships.

On February 14, 2023, the federal government announced its intent to further protect Canada's research, its institutions, and its intellectual property by announcing that Canada would adopt an enhanced posture regarding Canada's research security. The resulting new Policy on Sensitive Technology Research and Affiliations of Concern was developed in close consultation with implicated federal departments and agencies including Canada's federal granting councils – the Canadian Institutes of Health Research (CIHR), the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council of Canada (SSHRC) – as well as the Canada Foundation for Innovation (CFI), Global Affairs Canada (GAC) and Canada's research community through the Government of Canada-Universities Working Group.

In the development of this policy, Canada focused on ensuring that Canada's research ecosystem remains as open and internationally collaborative as possible, in alignment with its foundational principles of transparency, merit, academic freedom, and reciprocity. In so doing, this enhanced posture is meant to safeguard, but not limit, Canada's cutting edge research by mitigating research security risks. To appropriately protect Canada's research ecosystem, the Government of Canada will continue to work in close collaboration with Canada's research community, universities and our provincial and territorial government partners.

Starting in early 2024, research grant and funding applications submitted by a university or affiliated research institution to the federal granting councils and the Canada Foundation for Innovation 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. To support this, Canada is releasing two lists that provide clear, defined, and transparent guidance so that researchers can quickly and efficiently determine if these new requirements apply to their research.

First, the Government of Canada is publishing a list of Sensitive Technology Research Areas that support the development and advancement of new technologies. It will allow researchers to self-assess whether their proposed research is within the scope of this new requirement. Research that will merely use an existing technology is not within the scope of this policy.

Second, the Government of Canada is publishing a list of Named Research Organizations connected to military, national defence, or state security entities that could pose a risk to Canada's national security. This list was developed by Public Safety Canada and with experts across the federal government using a risk-based approach.

Canada's research security policies remain country-agnostic. Recognizing that threats evolve and can come from anywhere in the world, both lists will be regularly reviewed to keep pace with the latest developments in research and to ensure that we continue to address evolving risks in an increasingly complex geopolitical environment.

This policy will be implemented through an attestation by researchers that have a named role (for example, applicants co-applicants, and collaborators) as part of the grant / funding application process for research projects advancing sensitive technology research areas. The federal granting councils and the Canada Foundation for Innovation are developing procedures and guidance to implement this new policy. More detailed information on the implementation of the policy, including forms and procedures, will be published on their respective web pages in advance of the policy implementation.

While the policy will only come into effect as of early 2024, the Government of Canada may take research affiliations into account immediately as part of research funding decision-making processes, should risks be identified. In particular, research affiliations will be considered as part of the national security assessment of any research grant applications that are subject to the National Security Guidelines for Research Partnerships.

Canada recognizes that some research collaborations in sensitive technology research areas not involving connections to listed named research organizations may still present risks, and as such, researchers and institutions are encouraged to continue to exercise due diligence in all of their research partnerships, and to make full use of other research security tools available to them including those provided on the Safeguarding Your Research portal. Canada will also continue to encourage Canadian universities to implement a similar enhanced posture for all research partnerships and collaborations in sensitive technology research areas.

Principles

The development and implementation of the Policy on Sensitive Technology Research and Affiliations of Concern is guided by the following principles:

- Risk-targeted: the policy is based on evidence and focused on the most sensitive technology research areas and highest national security threats.
- Science appropriate: the policy minimizes impacts on Canada's research and research funding ecosystem by ensuring that it is as open as possible and as secure as necessary.
- Transparent: criteria and guidance are clear and openly accessible to the research community.
- Free from Discrimination, Harassment, and Coercion: this policy focuses on specific threats identified with regards to the military, national defence, or state security entities that could pose a risk to our national security; it does not target or profile any group of people or country.
- Collaboration with the research community: through continued dialogue and consultation-development of research security measures.

Definitions

Activities supported by the grant*:* Any contribution to research related to the funded grant and throughout the lifecycle of the research project(s), up to and including the dissemination of research results (e.g., publications).

Affiliation: Individuals are considered affiliated to any organization at which they are employed, appointed, or conduct research. In cases where individuals hold multiple affiliations, all must be identified and considered when ensuring compliance to this policy.

Funding and in-kind support: Monetary or non-monetary contributions, that include but are not limited to goods, equipment, materials and supplies, professional services, use of facilities (office space, lab access), software, technologies and databases.

Researcher: Any person conducting research activities. For the purposes of funding applications to the federal granting councils and the Canada Foundation for Innovation, researchers can hold different roles, including but not limited to applicants, co-applicants, collaborators, and highly qualified personnel (HQP). HQP can include undergraduate and graduate students, post-doctoral fellows, as well as research staff.

Sensitive technology research area: areas of research identified on the list of Sensitive Technology Research Areas*.* For the purposes of this policy, only projects in listed sub-categories of areas of research are considered sensitive and trigger an attestation requirement. Areas of research not covered by the sub-categories of the list are not currently considered sensitive for the purposes of this policy and therefore do not trigger an attestation requirement. Within the scope of this policy, research in a sensitive technology research area is not a concern on its own, unless it is conducted in affiliation with a research-performing institution of concern. Research in these areas with likeminded collaborators, partners, and institutions is strongly encouraged.

Universities, research institutes and laboratories connected to military, national defence or state security entities that could pose a risk to our national security: as defined by the list of Named Research Organizations. The list is a non-exhaustive inventory of universities, research institutions, or laboratories connected to military, national defence or state security organizations that could pose a risk to Canada's national security.

Steps for Researchers: How to Comply with the New Policy

To comply with this new policy, applicants must undertake a two-step process prior to applying for a grant / funding. Applicants are encouraged to complete the steps below well in advance of the grant application submission, in consultation with their institution's research grants office.

Step 1 : Determine whether your grant / funding will aim to advance any sensitive technology research area

Principal investigators (PIs) applying to any federal research grant funding opportunity offered by NSERC, SSHRC, CIHR or to funding offered by the Canada Foundation for Innovation must review the list of Sensitive Technology Research Areas to determine if their proposed research will aim to advance any of the listed areas.

- If the proposed research **will not** aim to advance any of the listed sensitive technology research areas, no further steps are required under this policy. Research that will merely use an existing technology is not included in this policy.

- If the proposed research **will** aim to advance any of the listed sensitive technology research areas, the following step must be followed whereby **all researchers with named roles** involved in the activities funded by the grant must attest that they are not affiliated with, or in receipt of funding or in-kind support, from any of the institutions on the list of Named Research Organizations.

Step 2 : Check researchers' affiliations

All researchers involved in the activities funded by a research grant advancing a sensitive technology research area must review the list of Named Research Organizations. If a researcher is affiliated with, or in receipt of funding or in-kind support, from one or more of the institutions on the list of Named Research Organizations, they must terminate these connections in order for the federal grant application process to continue. **Only currently held affiliations are of concern for this policy; past affiliations will not be considered**. For example, if an undergraduate student has previously studied or worked at a listed institution but has since left the institution and maintains no formal obligation to return to being affiliated with the listed institution, then they are not currently affiliated to that institution and do not raise a concern with regards to this policy.

If a researcher chooses to continue to be affiliated with, or in receipt of funding or in-kind support, from a listed institution, the grant application will not be eligible for federal funding. The grant application process can only proceed if the connection to the listed institution is terminated, or if the researcher in question is no longer part of the grant application. Moreover, researchers affiliated with, or in receipt of funding or in-kind support, from a listed institution cannot join a project once the grant has been awarded, unless they terminate these connections prior to joining the project.

All researchers with named roles engaged in activities supported by the research grant will be required to attest that they have read, understood, agree with, and are compliant with this policy. They and their research team(s) will be required to comply with the policy **for the duration of the federal grant**.

This new policy is focussed on researcher affiliations and targets the highest risk collaborations with military and state security-related institutions. As part of this policy, researchers should keep in mind that institutions that are not included on the Named Research Organizations list at this point in time may still pose a risk to Canada's research and 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. A suite of research security guidance and tools is available on the Safeguarding Your Research portal, including the National Security Guidelines for Research Partnerships which apply as a requirement to certain federal research partnership funding opportunities.

Validating Information: What Happens After Application

Federal research grant applications and Canada Foundation for Innovation funding applications will be periodically selected for a process to validate compliance with the policy.

Validation is expected to take place through one of two routes:

- For most federal research grant funding opportunities, validation will be conducted through a sampling of funded applications, on a regular basis within each granting council and the Canada Foundation for Innovation. This validation may be completed after grant funding has been awarded.

- For federal research partnership grant funding opportunities where the National Security Guidelines for Research Partnerships apply, validation of attestations will be completed in parallel for applications that are selected for national security assessment. In these cases, validation will occur prior to a funding decision.

The Government of Canada is committed to minimizing the impact of this new requirement on funding decision service standards.

The validation process will be actioned by national security departments and agencies in collaboration with the relevant funding organization(s).

If the validation process finds that a researcher has an undisclosed affiliation of concern, or is in receipt of funding or in-kind support from a listed institution, it will impact the researcher's eligibility to participate in the activities funded by a grant in a sensitive technology research area. Further action will be taken by the federal granting council and / or the Canada Foundation for Innovation to address the finding, pursuant to the organization's authorities and to the terms and conditions of the related grant(s).

Any misrepresentation by a researcher in a grant or funding application may constitute a breach of the Tri-Agency Framework: Responsible Conduct of Research (RCR). Following the RCR process, the Canadian institution that the researcher is affiliated with will be responsible for conducting an inquiry and (if warranted) an investigation of the allegation. Recourse for breaches of the RCR Framework varies by severity, intentionality, and impact of the breach, but may include and is not limited to: withholding installments of and/or termination of the grant; a requirement to reimburse funds; and ineligibility to hold/apply for federal funding, for a defined period of time or permanently.

For More Information

The federal research granting councils and the Canada Foundation for Innovation are in the process of implementing this new policy. More detailed information, including forms and procedures, will be published on their respective web pages in the coming months.

Applicants and research institutions are also invited to communicate with the Research Security Centre if they have further questions.