Universities Canada
Briefing Note on New Research Security Measures

Information included:

- Purpose
- Current Context
- Who is affected?
- Impact on institutions and researchers
- Support for institutions
- Precautions
- Key messages

Purpose

This document is intended to provide a general overview of the new research security lists that have been announced by the Government of Canada as it implements the Tri-Ministerial Statement on Protecting Canada's Research first announced in February 2023.

The Government of Canada remains the primary source for the full parameters of the new measures and how they will apply to specific research areas. We also encourage researchers to consult the accompanying FAQ provided by the government as it describes several scenarios regarding the applicability of the lists.

The government has also indicated that certain details for the policy may evolve over the coming months following feedback received from the community, including through the Government of Canada – Universities Working Group.

Current Context

- The Government of Canada has announced the creation of two lists:
  - the list of Sensitive Technology Research Areas (STRA)
  - the list of Named Research Organizations (NRO)
- The full policy will be referred to as the Sensitive Technology Research and Affiliations of Concern (STRAC).
- The two STRAC lists do not come into effect immediately. Once the policy comes into effect in Spring 2024 (exact date TBD), any research project that seeks to advance a Sensitive Technology Research Area in partnership with someone who is affiliated with a Named Research Organization will no longer qualify for new federal research grants until the affiliation with the Named Research Organization has been disentangled.
- These lists are evergreen in that they could be updated in the future. It is likely that the STRA will become more specific over time while the NRO could eventually include other research organizations.

- Following the Government of Canada's announcement of the development of these lists, Universities Canada has engaged with the government to ensure they consider the potential for unintended consequences, including:
    - Uncertainty and administrative requirements that can make research partnerships more difficult to establish and manage, even for partners not targeted by the lists.
    - Administrative burdens that could introduce new costs and pull the focus of researchers away from their research, which could be harder to navigate for smaller institutions without a research security office.
    - Discrimination towards ethnic groups associated with the lists: researchers may avoid hiring or partnering with specific ethnicities if there is a perception that compliance requirements will be more difficult and making a mistake could put future research funding at risk.
- The announcement of the lists brings clarity to uncertainty that followed the February statement. While many of the above concerns raised have been reduced, the concerns remain.
- This new policy is in addition to the existing *National Security Guidelines for Research Partnerships* which were piloted through the Alliance Grants funding stream at NSERC. These guidelines are still expected to expand to other funding streams for research partnerships.

Who is affected?

These are broad rules designed to give a quick overview on who will be affected by the new measures:

- This policy applies to federal funding opportunities administered by the tri-agencies (NSERC, CIHR and SSHRC) and the Canadian Foundation for Innovation (CFI) that fund research grants to universities and affiliated research institutions.
- The policy is not retroactive to grants received prior to the implementation of the new measures. However, existing projects that apply for an extension with additional funds must comply with the policy.
    - Applications submitted before the policy comes into effect are not subject to the policy.
    - Timed calls for proposals that opened before the policy comes into effect are not subject to the policy.
    - If the lists are updated after a grant application was submitted, the lists that were in effect at the time of submission will apply.
- Only researchers named on a federal grant application will need to provide the granting agencies with an attestation that they are not affiliated with, or in receipt of funding or in-kind support from, an NRO and that all research activities.
    - However, all research team members will need to comply with the affiliation requirements, including graduate students. Named grant applicants will need to attest that they understand that requirement.
- The STRA list only applies to research that **advances** research in a listed technology. Simply the use of the technology as part of a research project is not enough for the research project to be considered sensitive.
    - For example, even though Next Generation (genomic) Sequencing is listed in the STRA, projects that use the technology to sequence their samples should not need to attest that they are advancing a sensitive technology research area.

    - If a researcher is unsure whether their use of a given sensitive technology is advancing it, they should contract their institutions' research / research security offices for case-by-case advice.
- This process is not expected to cause delays in funding decision service standards as validation of compliance with the policy will occur on a random subset of applications after funding decisions have been made.
    - **Note:** For any funding opportunity where the National Security Guidelines for Research Partnerships apply, validation of attestations will be completed in parallel for applications selected for national security assessment. In these cases, validation will occur prior to a funding decision.

Impact on institutions and researchers

- For research that does not advance listed Sensitive Technology Research Area, researchers will simply need to check a box on their grant application and are not required to provide anything further, such as an attestation.
- If the research advances a listed STRA, all researchers with a named role on a grant application are required to submit an attestation stating that they are not affiliated with, or in receipt of funding or in-kind support, from a Named Research Organization.
- In the event that there is an alleged affiliation that is flagged by the Government of Canada, it may invoke an allegation of misrepresentation in an agency application or related document as per the Tri-Agency Framework: Responsible Conduct of Research (RCR).
- Following the RCR process, the researcher's institution will be responsible for conducting an inquiry and (if warranted) an investigation of the allegation.
- Efforts will be made with the implicated institution(s) to address the issue and to determine the best route forward to minimize impacts on the research and on the grant.
- ISED department officials have repeatedly indicated that researchers will not be penalized or have future funding put at risk if a member of their team fails to disclose an affiliation that they were not aware of. Recourse for breaches of the RCR Framework varies by severity, intentionality, and impact of the breach.

Support for Institutions

- The federal Research Support Fund provides many institutions with funding for research security, including for the creation of dedicated Research Security Offices. Unfortunately, many institutions are not eligible for these funds, and many that are eligible do not receive a workable amount of support. Universities Canada continues to advocate additional resources for these institutions, including increasing direct support through the Research Security Centre.
- As this document is a general overview, researchers and university administration looking for specific information on the policy should consult the government's documentation and the FAQ.
- While each institution will have their own process, in general researchers with questions about the policy and how it affects their research should contact their Research Security Office, or their Research Office in the absence of a Research Security Office.
- The *Research Security Centre* at Public Safety Canada has 6 regional advisors who have been establishing contact with each institution through their research/research security office.

- The expectation is that Research Security Offices will be able to answer most questions over time and establish their own processes. Meanwhile, the Research Security Centre is the point of contact for research/research security offices for advice when they don't have the answer.
- The University of Calgary, University of Toronto and University of Waterloo have led in the creation of the Team Canada initiative, which convenes research security directors and others with research security as part of their mandate. Presently, there are nearly 40 institutions involved in this forum to discuss current issues and best practices and Toronto Metropolitan University is leading a sub-committee focused on small and medium-sized universities and their needs.

Precautions

- Although the government has indicated that the NRO list was developed to be country agnostic, it's unclear how countries with institutions featured on the list may react.
- As a matter of due course, it is always recommended that Canadian researchers work with any travel security procedures put in place at their institution, consult travel advisories and register with Global Affairs Canada when travelling abroad. Researchers are also encouraged to consult the Travel Security guide for university researchers and staff that was codeveloped by Universities Canada and U15.

Key Messages

- International partnerships are essential for Canada to remain competitive on the world stage. Research and technology transfers work both ways, and Canada benefits greatly from building on the progress being made elsewhere in the world.
- Universities recognize that collaborations can sometimes carry risk or raise national security considerations, and are taking active measures to mitigate such risks without harming important research progress.
- Canada's universities welcome the clarity that these lists add to the Government of Canada's February statement on research security, which complement the work that universities have been doing over the years to strengthen research security measures, including:
    - Creating research security offices;
    - Developing the Research Security Guidelines on Research Partnerships;
    - Limiting partnerships of concern;
    - Raising risk awareness; and
    - Travel security measures.
- Given that federal research funding has stagnated over the past two decades, the Government of Canada must couple these measures with supports to ensure that the critical research identified in these lists can continue in Canada, so that projects are not abandoned completely in the absence of research partners or grants.
- If the government closes the door to some research collaboration without opening others, they risk driving talent and IP out of Canada. Acknowledging this, peer countries have coupled new research security policies with new research opportunities:
    - The American CHIPS and Sciences Act introduced very targeted restrictions that were complimented with significant research investments.
    - The Australian list of critical technologies is a list of opportunities the country wants to promote, including with other peer nations, while developing more robust risk mitigation practices.

- The government needs to also ensure smaller institutions and institutions with an increased focus on sensitive research are not left out of security initiatives such as the Research Support Fund.
- It's important that the government sends a clear message that, outside of limited areas of increased risk, we need to maintain robust international research collaborations to remain competitive and attract new ideas and talent.
- The government needs to work with the research community to ensure that talented researchers are not discriminated against based on nationality despite meeting the necessary security requirements.

Additional remarks

- While Universities Canada and other members of the Government of Canada – Universities Working Group have provided feedback on specific issues concerning the policy's development, we are now assessing the full details of the announcement. We will continue to engage with the Government of Canada as issues with the policy and its implementation emerge. Questions and feedback regarding our research security engagement with the federal government can be sent to shughes@univcan.ca.