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

FACULTY OF SCIENCE | MEMORIAL UNIVERSITY

July 10th 2024, **On the Menu**

Land Acknowledgement

"We acknowledge that the lands on which Memorial University's campuses are situated are in the traditional territories of diverse Indigenous groups, and we acknowledge with respect the histories and cultures of the Beothuk, Mi'kmaq, Innu and Inuit of this province."

National Security Guidelines for Research Partnerships

- Introduced in 2021
- Integrates national security considerations into the development, evaluation, and funding of research partnerships
- Applies to **NSERC Alliance Program** with **Private Sector Partners**
- Risk Assessment Form completed as part of the application
- Risk, and risk mitigation plan if applicable, assessed during grant review

RESOURCES:

- Guidelines (PDF)
- VIDEO

Sensitive Technology Research and Affiliations of Concern (STRAC)

- Evidence based policy focused on protecting Canada's research in the most sensitive areas from national security threats
- Announced by federal government in Feb. 2024, policy came into effect May 2024
- Utilizes two separate lists which operate in conjunction:
  - Sensitive Technology Research Areas (STRAs)
  - Named Research Organizations (NROs)
- Research that advances technology in a STRA will not be funded if 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

Strategic Technology Research Areas (STRA)

1. Advanced Infrastructure Technology
2. Advanced Energy Technology
3. Advanced Materials and Manufacturing
4. Advanced Sensing and Surveillance
5. Advanced Weapons
6. Aerospace, Space and Satellite Technology
7. Artificial Intelligence and Big Data Technology
8. Human-Machine Integration
9. Life Science Technology
    1. Biotechnology
    2. Medical and Healthcare Technology
10. Quantum Science and Technology
11. Robotics and Autonomous Systems

Medical and Healthcare Technology

Medical and healthcare technology refers to tools, processes or services that support good health and prevent, or attempt to prevent, disease. Advances in biotechnology, nanotechnology and advanced materials are enabling new methods of delivering medicine or treating injuries, diseases or exposure to toxic substances.

Chemical, Biological, Radiological and Nuclear (CBRN) medical countermeasures

Various medical assets used to prevent, identify or treat injuries or illnesses caused by chemical, biological, radiological or nuclear (CBRN) threats, whether naturally-occurring or engineered. CBRN medical countermeasures include therapeutics to treat injuries and illnesses, such as biologic products or drugs, as well diagnostics to identify the threats.

Gene therapy

Use of gene manipulation or modification in humans to prevent, treat or cure disease, either by replacing or disabling disease-causing genes or inserting new or modified genes.

Nanomedicine

Use of nanomaterials to diagnose, monitor, prevent and/or treat disease. Examples of nanomedicine include nanoparticles for targeted drug delivery, smart imaging using nanomaterials, as well as nano-engineered implants to support tissue engineering and regenerative medicine.

Tissue engineering and regenerative medicine

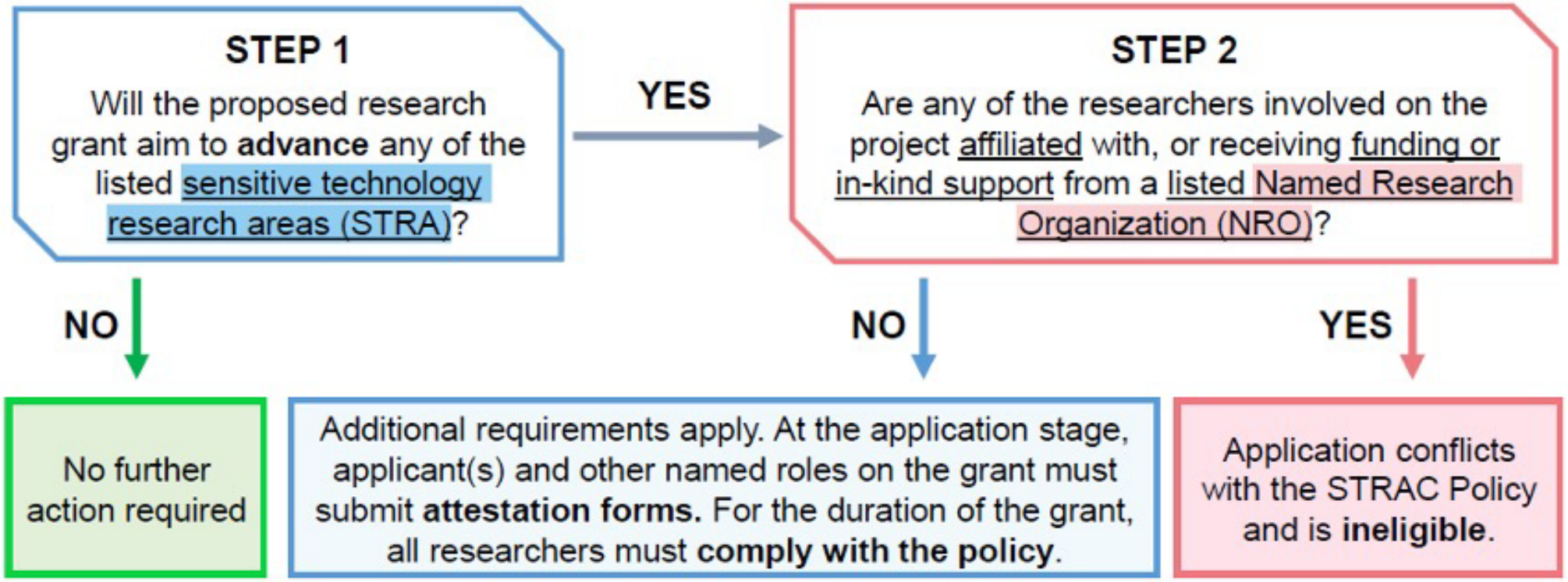
Methods of regenerating or rebuilding cells, tissues or organs to allow normal, biological functions to be restored. Regenerative medicine includes self-healing, where the body is able to use its own tools or other biological materials to regrow tissues or cells, whereas tissue engineering largely focuses on the use of synthetic and biological materials, such as stem cells, to build function constructs or supports that help heal or restore damaged tissues or organs.

Named Research Organizations (NRO)

- Research Organizations and Institutions which pose the highest risk to Canada's national security due to direct, or indirect connections with military, national defence, and state security entities
- 103 NROs
- Best Practice: apply due diligence to assess any new collaborations

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:



Attestation for Research Aiming to Advance Sensitive Technology Research Areas

Date of attestation (yyyy-mm-dd)

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.

Responsibilities of the PI

- Determining if the proposed research aims to advance a STRA
  - Tri-agency security team can help if you are unsure
  - Policy not applicable to technology that may already be ubiquitous in the course of a research project
- Ensuring all team members are aware of the STRAC policy and their requirement to comply for the duration of the funding (including HQP)
- Ensuring the accuracy of your own attestation
- Inform Memorial and the funding agency if:
  - the proposed research changes such that it includes a STRA that was not previously identified
  - a new team member (named role) is added to your project which aims to advance a STRA

Validation of Policy Compliance

- Granting agencies will conduct periodic reviews on a randomized set of funded* applications
  - Determine if research is appropriately identified as aiming to advance a strategic research area
  - Determine if all researchers have any undisclosed affiliations of concern
  - Attestation form and abstracts will be shared with national security departments for assessment

* Applications under the National Guidelines for Research Partnerships will be Assessed at the time of application (e.g., NSERC Alliance)

Things to keep in mind

- The STRAC policy only impacts NEW grant applications
  - In effect for entire duration of grant including dissemination
- The STRA and NRO lists are not static
  - Researchers are only bound to the lists which were active at the time of their application
  - Federal funding agencies will try not to update lists immediately prior to major funding deadlines
- While HQP who are not named in a grant application are not required to submit an attestation, they are expected to comply with the policy
- You CAN include team members who were previously associated with a NRO, but are no longer affiliated (e.g., a student who graduated from an NRO but is no longer affiliated)
- This policy is new and evolving

Tips for Best Practice

- Save a copy of the STRA and NRO at the time of your grant application
- Save a copy of an attestation for all researchers who are working on the project (students, postdocs, staff, collaborators, etc.)
- If you are unsure as to whether your research would be considered as aiming to advance a STRA we recommend you reach out to the Tri-agency security team for guidance
- If you have recently terminated your affiliation with an NRO- maintain a record of that termination (e.g., resignation letter, emails from colleagues acknowledging your departure)

Resources

- STRAC Policy
- Sensitive Technology Research Areas list
- Named Research Organizations
- Safeguarding your Research
  - Safeguarding Science Workshops (synchronous & asynchronous)
- FAQs
  - Gov't of CAN
  - Tri-Agency

Contacts:

- **NSERC**: researchsecurity@nserc-crsng.gc.ca
- **CIHR**: support-soutien@cihr-irsc.gc.ca
- **SSHRC**: researchsecurity-securiterecherche@sshrc-crsh.gc.ca
- **Atlantic Regional Advisor on Research Security**: Beth.Cainen@ps-sp.gc.ca (782-409-5248)