Toronto Academic Health Science Network

GENERAL GUIDELINES FOR THE PROCESS OF MITIGATING SECURITY RISK IN RESEARCH ACROSS TAHSN

Developed by: A Working Group of the TAHSN Research (TAHSNr) Committee
Version Date: May 9, 2024

PURPOSE

To provide common guidelines to TAHSN institutions and their respective research institutes (referred to as 'TAHSN institutions' in this document), as applicable, and to help guide the process around appropriately mitigating security risk in research, in compliance with Canadian regulatory and funder requirements, and with an understanding of the requirements in other jurisdictions.

This document provides a set of recommended guidelines that each institution is encouraged to consider and incorporate into their processes and governance. The guidelines are intended to be applied by each institution according to their own capacity and risk tolerances.

This document will need to evolve to reflect the changing Canadian regulatory and funder requirements.

BACKGROUND

In 2021, the Government of Canada ("GC") introduced National Security Guidelines for Research Partnerships ("Partnership (NSGRP) Guidelines") and piloted mandatory application of the Partnership Guidelines and completion of the GC's Research Partnership Risk Assessment Form with a subset of Tri-Agency grants, with the expectation of future expansion to all Tri-Agency grant applications. In 2023, the GC announced an expansion of these Partnership (NSGRP) Guidelines to other Tri-Agency grants involving a private sector partner, with timeline and scope to be determined at a later date.

In 2022, the TAHSN Research (TAHSNr) Committee identified differences in the approach to research partnership security across TAHSN institutions which may interfere with collaboration efforts across TAHSN. To address this, nominated research leaders from each TAHSN institution formed the *Research Partnership Security Working Group* ("Working Group.") The purpose of the Working Group was to develop a coordinated approach that aligns tools and considerations across TAHSN, while allowing institutions the flexibility to implement security reviews according to their capacity and risk tolerances. The goal of this approach is to limit workload for researchers and institutional review staff while promoting concurrence between institutions.

In the interest of improving alignment where appropriate and fostering collaboration, this Working Group harmonized supporting documentation, forms and processes (each where possible), which will be used to evaluate and mitigate security risk in research partnerships, in compliance with GC Security Policies. In terms of the Partnership Guidelines, the Working Group harmonized the Research Partnership Security Information Document for International Partnerships used by researchers to assess partnership risk, and developed common guidelines on how to use this form.

In February of 2023, the Government of Canada announced its intention to further expand its focus on national security risk, by specifically addressing concerns around affiliations of concern by individual researchers working in sensitive technological areas that could compromise national security interests. GC introduced a separate policy entitled Policy on Sensitive Technology Research and Affiliations of Concern ("Affiliation (STRAC) Policy") in January of 2024. This new Affiliation Policy will come into effect in Spring of 2024.

In response to these policies, the Working Group expanded its mandate to encompass a similar goal of harmonizing supporting documentation, forms and processes (each where possible) to evaluate and mitigate security risks in respect of researcher affiliations in compliance with the Affiliation (STRAC) Policy in the interest of improvement alignment where appropriate and fostering collaboration.

The Working Group has also expanded its mandate to encompass a similar goal of harmonizing supporting documentation, forms and processes (each where possible) to evaluate and mitigate security risks in accordance with the guidelines and mandates implemented by the Ontario Government, which appears currently to be a separate, but partially overlapping approach to the policies of the GC.

CONSIDERATIONS

These TAHSN guidelines reflect consideration and incorporation of the global geopolitical landscape, and announcements in research security policies and guidance from each of the Government of Canada and the Government of Ontario. The purpose of these guidelines is to support compliance with current requirements from the Canadian and Ontario Governments and Canadian and Provincial funding agencies, including the Tri-Agency.

The focus of the guidelines is to support compliance with Canadian and Provincial regulatory and funder requirements. However, the considerations, resources and tools may support institutions in meeting requirements from foreign bodies such as for example the National Institutes of Health (NIH) in the United States.

Institutions have the flexibility to apply common tools and principles , however, this falls outside the scope of the current guidelines.

The TAHSNr Information Security Working Group is working with the Research Security Working Group to address issues related to cybersecurity.

RESOURCES

- The University of Toronto's (U of T) webpage on safeguarding research https://research.utoronto.ca/safeguarding-research/safeguarding-research
- U of T's Research Partnership Security Information Document for International Partnerships https://redcap.utoronto.ca/surveys/?s=PMF483RY8NMNNDJL
    - The Research Partnership Security Working Group is working on expanding the use of a more generally applicable and agreed-upon form to the TASHN community

- Policy on Sensitive Technology Research and Affiliations of Concern (STRAC) https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern
- Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy) https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/strac-rtsap_eng.asp
- Canada Foundation for Innovation (CFI) Approach to Research Security https://www.innovation.ca/apply-manage-awards/resources-apply-manage-award/research-security?_cldee=73sNkYjUizUtWRIvEq69a4xpksjqD-ZvAi_wukJIejjYsp0y6rEZhqbwrWW-iGEZ&recipientid=contact-f0e1c6da104ce811a95b000d3af451b4-26a011e25b8948cb8a4d815112450c02&esid=061963c3-89eb-ee11-a1fd-0022483dce9b
- National Security Guidelines for Research Partnerships (NSGRP) https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships
- Tri-agency guidance on the National Security Guidelines for Research Partnerships (NSGRP) https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp
- Mitigating Economic and/or Geopolitical Risk (MEGR) https://forms.mgcs.gov.on.ca/en/dataset/on00352
- Government list of training resources*:*
    - https://www.cyber.gc.ca/en/education-community/learning-hub/courses/620-introduction-research-security
    - https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/research-security-training-courses
    - https://learning-apprentissage.ised-isde.canada.ca/enrol/index.php?id=21
- U of T's webpage on International Research Security Standards https://research.utoronto.ca/international-research-security-standards
- US National Institutes of Health (NIH) Foreign Interference webpage https://grants.nih.gov/policy/foreign-interference.htm

ASSUMPTIONS

For the purpose of this document, it is assumed that:

- The scope of mandatory institutional partnership reviews is at the level of the international research partner on a per-project basis.
- The scope of mandatory reviews regarding researcher affiliations in compliance with STRAC is also on a per-project basis – but compliance obligations fall on researcher(s), with educational support provided at an institutional level.
- All TAHSN institutions have research governance and processes and the capacity to incorporate the guidelines
    - All TAHSN institutions will conduct reviews where mandatory (e.g. because service provider paid by Tri-Agency money)
    - Scope of institutional review beyond mandatory requirements is at the discretion of the institutions, who can use shared principles and tools to facilitate discretional reviews.

- TAHSN institutions have a shared responsibility and accountability for multi-institute collaborations
- One of a research institution's principal responsibilities is to protect public welfare
- It is important to appropriately balance security concerns with the researchers' rights to academic freedom

GUIDING PRINCIPLES

- **Principles of Research Security:**
  - Country agnostic, free from ethnic, racial and/or nationality bias
  - Maintain academic freedom
  - Maintain access to global talent
  - Promote the reputation of the TAHSN institutions and the University
  - Compliance with funder requirements

- **International research partners are evaluated based on their governing jurisdiction's requirements and systems of governance, per the evaluating institution's capacity and knowledge**

- **There should be no interference with researchers choosing their field of research/study**

- **International Research Engagements are transparent, purpose-driven and mutually beneficial**
  - Researchers and research institutions should consider - in any collaboration - risks to the Institution and the University, national interests, national security, reputation, financial risk and misuse or maligned use of research results or intellectual property
  - International Research Partners are evaluated for connectivity to a foreign military, security or intelligence, government's objectives, taking into account how those objectives could undermine Canadian objectives, and further taking into account the country's level of compliance with the rule of law
  - Researchers and research institutions should understand to fullest extent possible the organization (including beneficial ownership) with which they want to partner, including its governance structure, funding, and any implications these details may have
  - Researchers should understand the person and the specific area/subdivision (lab, school, etc.) within the international research partner organization that they are working with
  - The specific purpose of the partnership must be clear, and data disclosed during a partnership will be focused and appropriate to answer specific research hypotheses, both scientifically and ethically. This does not prevent generating new ideas during the partnership, for later exploration through established processes at the institutions.
  - Researchers will be able to articulate the value; value is not always financial in nature and can include the advancement of research interests, patient care and/or education

- **Risk Proportionality:** Response to risks should be proportionate and appropriately scaled. Each TAHSN institution should determine how to appropriately scale risks responses for their

International Research Partnerships, and how they are addressing Researcher Affiliations, and each should take into account the potential for misuse of the research and the aggregate level of risk, as well as the appropriate allocation of risk as between the TAHSN institution, and the researchers under their auspices, taking into account the government requirements. Higher levels of risk should require more senior levels of decision

- **Where possible and practical, research institutions across TAHSN will share common resources and definitions, i.e.:**
    - See 'resources' section on page 2
    - See 'definitions' section on page 2
    - Shared educational resources

- **A research institution has the responsibility to ensure its staff are educated and up to date on the most current national security guidelines:**
    - **Training:** Creating training/certifications for staff accessing protected assets, depending on level of authority and proximity to the asset.
        - Expose staff to government-provided training as applicable
    - **Awareness:** Staff should be continually made aware of processes put in place to assist in protecting public welfare, through reminder posters, announcements etc.

- **Each TAHSN institution has the responsibility to establish roles to ensure processes are established and followed per the mandatory requirements. The following roles are recommended across TAHSN for consideration:**
    - **Protecting data infrastructure**: A role that ensures digital assets are protected and provides guidelines for safe usage of data to staff (e.g. I.T. Director, office of the CISO)
    - **Partner evaluation**: A role that evaluates International Research Partnerships engaged in by scientists, ensuring only reputable partners have access to protected assets (research, data, equipment etc.), and creating the guidelines for staff on those international research partnerships
    - **Communication:** The role of the institution is to enable communications and provide support to researchers in understanding the implications of research security requirements, especially those in NSGRP, STRAC and Ontario. Institutions are to provide a completeness check to ensure that all required documents are complete, but are not specifically expected to validate the accuracy. Where possible, institutions may support their grant recipients in following best practices. Researchers exercise the ongoing responsibility of being aware of the research funding requirements, including research security provisions.

PROCEDURAL IN-SCOPE ACTIVITIES

- Coordinated operational review process to support researchers in navigating research security requirements for each funding application.

- Consideration of researcher and partner affiliations, including domestic and international academic partners, and corporate partners and their named co-investigators.

FUTURE DIRECTIONS

Canadian regulatory and funder requirements continue to evolve and the Working Group will continue to monitor the environment and respond to evolving regulations as they emerge.

- The initial scope of the Working Group was limited to the international research partner, on a per-project basis. The scope of mandatory research security reviews may expand to meet evolving requirements which may include the affiliations of TAHSN researchers.
- The Working Group will continue to meet and monitor the changes to the scope and how to appropriately expand the scope of the guidelines.
- The Working Group also has connections to an established provincial group, dedicated to research security, which will help inform changes and provide information on the government's due diligence processes and decision-making.
- The TASHN community is in discussion with U of T on how to best provide research security services and scope.

Toronto Academic Health Science Network

APPENDIX – OVERVIEW OF GRANT RESEARCH SECURITY PROCESSES

Contents

National Security Guidelines for Research Partnerships (the Guidelines / NSGRP)

1. Brief Intro; current programs/ expansion likely – always check funding opportunity announcement and institutional requirements

At present, the National Security Guidelines for Research Partnerships (NSGRP) risk assessment process applies to Natural Sciences and Engineering Research Council of Canada (NSERC) Alliance and Canada Foundation for Innovation (CFI) Innovation Fund applicants who are working with a private sector partner. In fall 2024, the NSGRP process will be expanded to the Canadian Institutes of Health Research (CIHR) Project Grant and NSERC Idea to Innovation Grant applicants.

When granting agencies conduct national security reviews, they will analyze all partners and all listed individuals identified on the application. Likewise, when conducting bibliometric reviews, granting agencies may consider all co-authors on a paper.

Funding opportunities will identify when NSGRP applies, and risk assessment forms will be included with the funding application document package.

2. Definitions

- **Research Partner (“or “Partner):** an entity (e.g., academic, corporate, government or not-for-profit) that is engaged with a TAHSN institution in a research collaboration (which may also include graduate training and/or entrepreneurial opportunities) and that is located either within or outside of Canada, inclusive of beneficial ownership.
- **Research Security:** To address and provide advice on institutional geopolitical risks and identify and mitigate any potential risks related to research in partnerships

3. Re-state Guidelines link (direct to landing page not to Safeguarding Your Research Page)

- National Security Guidelines for Research Partnerships
- Tri-agency guidance on the National Security Guidelines for Research Partnerships (NSGRP)

Sensitive Technology Research and Affiliations of Concern (STRAC)

1. Brief Intro (as above)

On January 16, 2024, the Government of Canada released a new Policy on Sensitive Technology Research and Affiliations of Concern (STRAC). To be eligible to receive new research funding in a Sensitive Technologies Research Area (STRA) from any of the Tri-Agencies (Canadian Institutes for Health Research (CIHR), Social Sciences and Humanities Research Council (SSHRC), Natural Sciences and Engineering Research Council of Canada (NSERC) and the Canada Foundation for Innovation (CFI)), each researcher listed on a research funding application must provide an individual attestation that they do not have any affiliations with or are not in receipt of funding or in-kind support from entities on the Named Research Organizations (NRO) list.

Tri-Agency funding for projects on the STRA list will not be granted if a listed researcher has an affiliation with a named research organization. Implementation will begin in spring 2024 so that researchers can end current affiliations of concern before applying for a Tri-Agency grant.

2. Definitions

- **Affiliation:** Individuals are considered affiliated to any organization at which they are currently employed, appointed, receive financial benefits 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. At CIHR, 'Researcher' specifically includes the Nominated Principal Applicant, Principal Applicants, Co-Applicants, Principal Knowledge Users, and Knowledge Users. It does not include Collaborators as their role differs significantly for CIHR compared with the other funding agencies. Other members of the research team not playing one of the applicant roles above (including, for example, graduate students, post-doctoral fellows, research staff, etc.) are not required to complete an attestation form but must be considered in terms of ongoing policy compliance.
- **Sensitive technology research area:** areas of research identified on the list of Sensitive Technology Research Areas. For the purposes of STRAC, 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 STRAC, 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.

- **Named Research Organization:** A research organization or institution that poses a high risk to Canada's national security due to their direct or indirect connections with military, national defence, and state security entities.
- **Advancing:** The decision to determine whether research counts as 'advancing' is up to the researcher's discretion to determine. If the researcher does not identify a technology as 'advancing' but the government does, the researcher will be asked to complete an attestation form.

3. Re-state Guidelines link (direct to STRAC)

- Policy on Sensitive Technology Research and Affiliations of Concern (STRAC)
- Sensitive Technologies Research Area (STRA)
- Named Research Organizations (NRO)
- STRAC FAQs
- Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)
- Canada Foundation for Innovation (CFI) Approach to Research Security

Toronto Academic Health Science Network

Ontario Research Fund (ORF)

1. Brief Intro

In Ontario, applicants are required to complete the Mitigating Economic and Geopolitical Risk Checklist for Ontario Research Fund Applications related to research security for funding programs delivered through the Ministry of Colleges and Universities (MCU). These include Ontario Research Fund (ORF) programs: Large/Small Research Infrastructure (CFI matching) and Research Excellence (research operating grants).

- New: for the next 2024, and subsequent Ontario grant calls, researchers will be ask to specifically attest if they have any "Active Collaboration" with entities on Federal the Named Research Organizations (NRO) list, inclusive of co-authorship and co-publication. This is not an eligibility requirement: you can indicate yes (affiliated), contextualize the collaboration in the geopolitical checklist form and still potentially win your grant.
- The Ontario definition of Active Collaboration is different than the Federal definition of Affiliation. An Active collaboration is a material collaboration in most cases within two years of submission, which implies scientific collaboration, including but not exclusive to co-author, co-publication, joint research, or joint funding recipients.

The required checklist also asks researchers to provide context regarding collaborations with partners, inclusive of co-authorship and co-publication in risk-based jurisdictions beyond the NRO.

The Provincial government will then assess the checklist for concerns from a research security perspective. While the government analyzes all listed partners, including those beyond named researchers and individuals on an application, it does not provide a publicly available list of partners of concern. The provincial government's attestation process normally includes collaborations going back approximately two years to ensure that they are no longer active.

Prior to rendering a funding decision, the government will provide institutions the opportunity to address identified research security concerns by providing additional context or mitigation strategies. This information is provided through an official attestation document.

2. Definitions

Active: A material collaboration in most cases within two years of submission.

Collaboration: Implies scientific collaboration, including but not exclusive to co-author, co-publication, joint research, or joint funding recipients