National Security Guidelines for Research Partnerships (NSGRP)

Guidance on Completing the Risk Assessment Form

November 2024 Edition

Research Security Team

Email: researchsecurity@utoronto.ca
Website: Research Security: Safeguarding Research

UNIVERSITY OF TORONTO

DEFY GRAVITY

Table of Contents

A. Introduction

The Government of Canada's (GoC's) **National Security Guidelines for Research Partnerships (NSGRP)** integrate national security considerations into the development, evaluation and funding of research partnerships. They help prevent foreign interference, espionage and unwanted knowledge transfer that could contribute to the military, security and intelligence capabilities of states or groups that pose a threat to Canada or that may enable the disruption of the Canadian society, economy and critical infrastructure. These guidelines position researchers, research organizations and Government funders to undertake consistent, risk-targeted due diligence of potential risks to research security.

The **Risk Assessment Form** accompanies the NSGRP to assess potential risks that research partnerships may pose to Canada's national security and guide the development of effective mitigation measures. **This form is required for applications to several Tri-Agency and CFI research funding programs involving one or more partner organizations from the private sector. Only one Risk Assessment Form is required per application, regardless of the number of partners.**

Read this Introduction in full before filling out the Risk Assessment Form. Sections B and C of this guide are designed to be consulted as you complete the form.

Tips for Completing the Risk Assessment Form

- **Complete the Entire Form:** All questions on the Risk Assessment Form must be answered. Any missing responses will result in the form being deemed "Incomplete" and the funding application returned without further review.
- **Use the text boxes to justify your responses:**
    - All "Yes" or "Unsure" responses in Sections 1 and 2 must be addressed in Sections 3 and 4.
    - If you answer "No" to all questions in Section 1 and 2, you are still required to complete Sections 3 and 4, explaining your reasoning.
    - Regardless of how you answer Sections 1 and 2, use Section 4 to address relevant suggested areas that are highlighted on Page 5 of the Risk Assessment Form.
- **It's Okay to be Unsure:** "Unsure" is a valid response to questions that have no clear-cut "Yes" or "No" answer, provided you justify the answer in the text boxes in Sections 3 and 4.
- **Individualize Your Responses:** When responding to Sections 3 and 4, craft responses that reflect the unique context of the partners and project. Existing institutional policies and procedures may form part of the response, but they must be contextualized in relation to your project.
- **FAQs:** Tri-agency guidance on the NSGRP provides answers to frequently asked questions and is routinely updated.

Section 3: Identifying Risks

In Section 3, you must identify and explain the associated risk factors to all "Yes" or "Unsure" responses to the questions in Sections 1 and 2. Reviewers are looking for evidence that you have seriously considered any risks to the research and any risks posed by the outcomes of the research.

When identifying risks to your research, consider:

- Unauthorized access to materials, technology, or sensitive or unpublished data by malicious external actors
- Unauthorized or unintended sharing of materials, technology or data with partners of your private sector partners
- Accidental mishandling or improper use of goods or equipment, or failure to comply with security procedures by a member of a research team

Best practices for completing Section 3:

- Reference the question numbers from Sections 1 and 2 when outlining the potential risks.
- Answer in complete sentences in paragraph format.
- Include detailed examples of the risks and explicitly identify the potential severity of the impact should the risks occur. Provide an explanation of your assessment, even if you determine the identified risks are unlikely to occur or assess the potential severity of the impact as low.
- Include information about the reasoning or methods used to assess the risks.

Section 4: Developing Risk Mitigation Plans

In Section 4, describe mitigation measures that will address the risks identified in Section 3 **as well as** the suggested areas identified on Page 5 of the Risk Assessment Form or any additional areas you identify as relevant based on the proposed nature of your project.

Best practices for completing Section 4:

- Use bold subheadings that describe each mitigation measure in order to structure your response.
- Answer in complete sentences in paragraph format.
- Develop mitigation plans for all identified risks, even if they are unlikely to occur.
- Provide an implementation timeline and describe how mitigation tactics will be monitored for effectiveness.

For additional examples of mitigation tactics, review the GoC's Mitigating Your Research Security Risks.

Support from the Research Security Team

Contact the Research Security Team if you require assistance at any point during the completion of the Risk Assessment Form. Services provided by the Research Security Team include:

- Providing feedback on Risk Assessment Forms prior to submission
- Conducting due diligence on private sector partners and associated participants
- Providing guidance on how to answer questions related to the GoC's Sensitive Technology Research Areas (STRA) list in Q.1.6.

B. Know Your Research

Q.1.1: Are you working in a research area that is related to critical minerals, including critical mineral supply chains, on the Critical Minerals List?

When answering this question, consider:

- When the critical minerals are only incidental to the project (e.g., their potential presence in mine tailings or slurry) or are chemicals used in the project, answer “Yes” or “Unsure.” Provide an appropriate rationale with the risk identification.

When developing your Section 3 Risk Identification response:

- Provide details on which critical minerals are applicable and the nature of the research.
- Discuss economic or safety risks posed by the misuse or unauthorized acquisition of the critical minerals or proposed research.
- Consider whether the quantity of critical minerals in use may influence any potential risk.
- Highlight how benefits to the Canadian natural resources sector resulting from the research will outweigh identified risks.

When developing your Section 4 Risk Mitigation Plan:

- If safety risks are identified, discuss all transportation, use or storage safety measures that will be taken to reduce these risks.
- If economic risks are identified, discuss all site access or data control measures that will be implemented to reduce unauthorized access to the research.

Q.1.2: Are you working in a research area that is classified within one of the critical infrastructure sectors of the National Strategy for Critical Infrastructure?

When answering this question, consider:

- The National Strategy for Critical Infrastructure not only addresses the protection of infrastructure itself but also the protection of sensitive information that could pose a risk to infrastructure if inappropriately released.

When developing your Section 3 Risk Identification response:

- Describe which critical infrastructure sectors are applicable to your research and provide details on the nature of the research.
- Identify risks posed to Canadian infrastructure or associated sensitive information should bad actors gain access through the research activities.
- Highlight how benefits to the critical infrastructure sector resulting from the research will outweigh the identified risks.

When developing your Section 4 Risk Mitigation Plan:

- Explain plans for mitigation tactics such as controlled site access or data security and cybersecurity measures.

Q.1.3: Does this research project involve the use of personal data that could be sensitive?

When answering this question, consider:

- All research involving personal data is governed by the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2. (See Chapter 3 – The Consent Process and Chapter 5 – Privacy and Confidentiality).
- The research must receive approval by the appropriate U of T Research Ethics Board (REB). Contact U of T's Human Research & Ethics Unit for more information.

When developing your Section 3 Risk Identification response:

- Outline the source and nature of any personal data collected and/or accessed and the associated risks.
- Consider whether the risk level is impacted by how and where the data are stored.
- Consider the impact to the individuals if their personal data were accessed by an unauthorized party.

When developing your Section 4 Risk Mitigation Plan:

- Outline plans for data security, data sharing, restricted access, de-identification measures and other relevant details.
- Practices included in U of T's research ethics protocols (REB) and policies are sufficient mitigation tactics. Discuss how they will be applied in the context of your research project.
- Indicate whether REB approval is in process or if it has been secured.
- Outline how sensitive data will be managed and secured (e.g., encryption, multi-factor authentication, Canada-based servers, etc.).

Please contact U of T's Research Oversight & Compliance Office (ROCO) for additional support.

Q.1.4: Does this research project involve the development or use of large datasets that could be sensitive?

When answering this question, consider:

- Large datasets pose risks beyond personal data security (as covered by Q.1.3). Security measures may be required for commercial or geopolitical reasons.

When developing your Section 3 Risk Identification response:

- Outline the sources and nature of the datasets being accessed and the associated risks.
- Consider whether the risk level is impacted by how and where the data are stored.
- Consider the impact if the data were accessed in full by an unauthorized party prior to intended release upon publication.

When developing your Section 4 Risk Mitigation Plan:

- Explain plans for data security, restricted access, de-identification measures and other relevant details.
- Outline key aspects of how sensitive large datasets will be managed and secured during the project (e.g. encryption, multi-factor authentication, Canadian-based servers, etc.).
- For specific language, reference U of T's Information Security Guidelines for data and cybersecurity best practices.

Additional information can be found on the university's Information Security website. For support with security research data, please contact Research Information Security.

Q.1.5: Are you working in a research area that is related to goods or technology that are included on the Export Control List (ECL) of the Export and Import Permits Act (EIPA)?

When answering the question, consider:

- If the research involves working with items that are included on the ECL, **you must answer "Yes" to this question**, even if you do not plan to export these items from Canada.
- Exports can include the return of loaned equipment, repairs of equipment, exchanges of samples and specimens, and the transfer of instructions, test results and preliminary findings.
- Intangible transfers of software and technology, such as through e-mail or the cloud, are also subject to requirements of the EIPA.

When developing your Section 3 Risk Identification response:

- Identify the specific goods or technology that are included on the ECL.
- Identify whether you intend to export the goods or technology outside of Canada, and if so, who is responsible for managing the export (e.g., U of T, a private sector partner, or a third party).
- Identify whether the private sector partner will have access to the goods or technology.
- Consider whether factors such as the quantity or composition of the goods and technology, or the level of partner expertise with such materials may impact the risk.

When developing your Section 4 Risk Mitigation Plan:

- Explain relevant security measures, including data security or physical security practices, ensuring the proper handling and access of the controlled goods or technology.
- Identify any relevant permits.
- Identify any contact with U of T's Office of Environmental Health and Safety (EHS).

Contact U of T's Office of Environmental Health and Safety (EHS) for support.

Q.1.6: Are you working in a research area that may be considered sensitive or dual-use as listed in List 1 of Annex A of the National Security Guidelines for Research Partnerships?

When answering this question, consider:

- The purpose of this question is to determine whether the research could be considered sensitive if someone were to gain unauthorized access to the research. It also addresses whether the outcome of the research could have a military, intelligence or dual military/civilian application, regardless of whether that is intended use of the research.
- If you answered "Yes" to any of the preceding questions (Q.1.1 to Q.1.5) in the form **or** if you are conducting research identified on the GoC's Sensitive Technology Research Areas (STRA), you are working in a research area that could be considered sensitive or dual-use as per Annex A. **Answer "Yes" to this question.**

When developing your Section 3 Risk Identification response:

- Identify the research area in Annex A that is applicable to the proposed research, demonstrating to reviewers that you have considered the list.
    - If the STRA list applies, also identify the specific category and sub-category.
- Describe the worst-case scenario should the risk occur. Questions to consider include:
    - What is the worst thing that someone could do with the outcomes of this project?
    - What is the most damage someone could do if they gained unauthorized access to the resources supporting this research?
    - Assuming the existence of a bad actor, how could the research be misused, however unlikely?
- Identify the likelihood of each risk occurring, even if it is highly unlikely, and contextualize the assessment that led you to this conclusion.
    - For example, if you assess that the research could have a dual-use military application but that it would take too long to operationalize or be cost prohibitive for a malicious actor to misuse the research in such a fashion, explain your reasoning.
- Applicants may position the risks by highlighting how the benefit to Canada outweighs the risks.
- If you answered "Unsure" or "No" to this question, but your research is related to or could be reasonably misconstrued for technology on the STRA list, provide context for your answer.
    - For example, if you are using technology identified on the STRA list but not in a manner that meets the sub-category description (e.g., an imaging device with capabilities beyond those found in consumer-grade technology that **does not** provide a visual depiction of the physical structure of an object), state this in order to assist the external security reviewer who may not be an expert in your field.

When developing your Section 4 Risk Mitigation Plan:

- Explain mitigation strategies that will be put in place by both researchers and the private sector partner(s) to reduce the likelihood of the identified risks from occurring. This could include data and cybersecurity practices, site location access, relevant policies and procedures and training and consultation with relevant experts.

C. Know Your Partner

Q.2.1: Are there any indications that your partner organization(s) could be subject to foreign government influence, interference or control?

When answering the question, consider:

- This question (as well as 2.2) is far-reaching, prospective and may be difficult to answer definitively, especially for companies with global operations and numerous affiliates and subsidiaries that may not be publicly disclosed.
- Solicit input from your partner organizations and share the Risk Assessment Form with them. Critically assess and consider the information received from your partner when completing this question.
- Review available public sources of information about the partner (e.g., partner websites or other official materials, reputable news media, financial databases such as Pitchbook or Crunchbase).
- For a list of other considerations, review the Guiding Questions in U of T's Minimizing Risk When Establishing Partnerships.

When developing your Section 3 Risk Identification response:

- Work with your partner organizations to describe perceived or potential issues.
- Consider your partners' management structure, corporate partnerships and entities with beneficial or controlling ownership.
- For other tips and strategies on identifying risks, review:
    - *Safeguarding Your Research: What Are the Risks?*
    - The Non-Academic Partners checklist on page 8 of *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects*

When developing your Section 4 Risk Mitigation Plan:

- Work with partner organizations to identify relevant risk mitigation strategies based on the potential issues identified above. For example, this may include controlled access to the proposed research within the partner organization or providing details on the ownership and use of intellectual property generated by the research.

Q.2.2: Are there any indications that suggest a lack of transparency or unethical behaviour from your partner organization(s), that may impact the proposed research project?

When answering this question, consider:

- This information will be a matter of public record in most jurisdictions and should be easily located in a general web search or in reporting by reputable news sources.
- Soliciting input from partners on the most appropriate answer to this question.
- Focusing your response on the preceding five years and activities that have bearing on the research area.

When developing your Section 3 Risk Identification response:

- Work with your partner organizations to provide additional context on the issues and their relevance to the project.

When developing your Section 4 Risk Mitigation Plan:

- Work with your partner organizations to provide an appropriate mitigation plan.

Q.2.3: Are there any indications that an individual(s) involved in the research project from your partner organization(s) could have conflicts of interest or affiliations that could lead to unauthorized knowledge transfer?

When answering this question, consider:

- While this information may not be a matter of public record in most jurisdictions, any questions brought to your attention should be investigated. The individual's LinkedIn profile or publication history are a good place to start to identify connections that may require additional examination.
- Conflicts of interest or questionable affiliations may include, but at are not limited to:
    - Partnerships with entities on the GoC's Named Research Organizations list.
    - Organizations that are rated as "High" or "Very High Risk" on the Australian Strategic Policy Institute's Defence Tracker.
    - Participation in a foreign talent program.
    - Affiliation with a corporation that has been sanctioned by NATO countries (e.g., the Canadian sanctions list, the EU sanctions tracker, the US Office of Foreign Assets Control List and the US Bureau of Industry and Security Entity List).

Please contact the Research Security Team if you require assistance answering this question. It is recommended you contact the Team early in the application process with detailed information including names, contact information and, if possible, the resumes of the individuals from your partner organizations. This will help expedite the review.

During Section 3 Risk Identification and Section 4 development of a Risk Mitigation Plan:

- Work with U of T's Research Security Team to provide additional context on the issues, their potential relevance to the project and development of an appropriate mitigation plan.

Q.2.4: Are there any indications that as a result of this research project, your partner organization(s) will or could have access to your research institution's Canadian facilities, networks, or assets on campus, including infrastructure that houses sensitive data?

When answering this question, consider:

- Research partnerships may involve individuals or organizations visiting the university. This includes, but is not limited to:
    - Short-term visits to attend symposia or in-person meetings
    - Visiting scientists working at a university facility
    - Remote access to databases or file sharing environments.
- The issue of physical and cybersecurity related to data management is identified by funding agencies as an area requiring discussion.

When developing your Section 3 Risk Identification response:

- Specify the type of access the partner organizations may have to U of T's facilities, networks or assets and identify the type of risk posed by this access (e.g., unauthorized removal of sensitive equipment or materials, unauthorized access to research, personal data or other sensitive information).

When developing your Section 4 Risk Mitigation Plan:

- Describe how access to sensitive research areas, data and equipment is controlled and monitored with provisions for supervised access.
- If applicable, outline how remote access will be granted to IT environments, data and files.
- Review the Cybersecurity and Data Management checklist on page 9 of *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects* for best practice mitigation tactics.

For assistance with U of T's infrastructure protection requirements and services, contact Information Security.