National Security Guidelines for Research Partnerships Risk Assessment Form

Save As | Print | Reset

Family name of applicant:	Initial(s) of all given names of applicant:	Grant administering institution:

Introduction

The Risk Assessment Form is a tool to identify and assess potential risks that research partnerships may pose to Canada's national security as outlined in the National Security Guidelines for Research Partnerships and to develop effective mitigation measures.

In answering the Risk Assessment Form questions, you will provide information – to the best of your ability – that is specific to your proposed area of research and prospective research partner organizations. This information will be used to assess national security risks where the proposed research partnership could expose the research project to foreign interference, espionage or theft from foreign governments, militaries and other organizations, and also pose potential risks to the wider Canadian research enterprise.

For the purpose of the National Security Guidelines for Research Partnerships, a partner organization is any organization that plays an active role in the project and/or supports a research partnership through cash and/or in-kind contributions. Examples of a partner organization's role may include:

- Sharing in intellectual leadership or providing expertise;
- Active participation in research activities; and/or
- Application of research results and/or active participation in translating or mobilizing the knowledge produced to help achieve the desired outcomes of the project.

National security risks may be described as, but not limited to circumstances where there are potential instances of foreign interference, espionage, intellectual property theft or unauthorized knowledge transfer that:

- contribute to the advancement of military, security, and intelligence capabilities of states or groups that pose a threat to Canada; and/or
- disrupt the development of Canadian research and innovation, weaken the resiliency of critical infrastructure, or jeopardize the protection of sensitive data of Canadians.

The information collected will not be used to substantiate if you are compliant with any legislative or regulatory requirements that may apply to your proposed research project. The collection of this information will be used to assess the overall risk profile of your research project.

Who needs to complete the Risk Assessment Form?

Anyone can use the Risk Assessment Form to conduct due diligence when establishing and/or continuing partnerships with national, international and multinational partners.

This form may be required for specified federal research funding opportunities. You should consult the appropriate program literature associated with the funding opportunity to which you are applying to determine if you are required to submit a Risk Assessment Form with your grant application.

Depending on the specific funding opportunity, the "applicant" may be an individual, on behalf of any co-applicants, or may be a post-secondary or research institution.

What resources and tools may assist you?

You are encouraged to conduct open-source research to complete the Risk Assessment Form and to consult with your partner organization(s), where appropriate, to validate the information. For more information, consult the comprehensive guide Conducting Open Source Due Diligence for Safeguarding Research Partnerships.

Additional guidance and resources, including Public Safety Canada's Safeguarding Science Workshop and the Canadian Security Intelligence Service's threat briefing and checklist, that may assist in the completion of this form can be located on the Safeguarding Your Research portal.

Save As | Print | Reset

Save As | Print | Reset

Section 1: Know Your Research

The purpose of this section is to gather key information about your research. This information will be used to assess whether the nature and/or usability of your **research project** could attract the interest of foreign governments, militaries, their proxies, and other organizations who may seek to exploit research partnerships to access research information, research knowledge, and the resulting intellectual property and technology to facilitate unauthorized knowledge transfer.

Research areas that are sensitive or dual-use, in that they have military, intelligence, or dual military/civilian applications, are more likely to present national security risks.

Answers to the following questions will assist in determining the overall risk profile of your research project. Risk Assessment Forms are assessed on a case-by-case basis, and answering "yes" or "unsure" to any of these questions is not a determinant of a denial of funding. For more information on the risk assessment process, consult the Safeguarding Your Research portal.

Answer the following questions to the best of your ability by using information that can be reasonably accessed through open sources that are available to you.

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? ◯ **Yes** ◯ **No** ◯ **Unsure**

The Government of Canada has developed a list of minerals considered critical for the sustainable economic success of Canada and our allies and to position Canada as a leading mining nation.

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? ◯ **Yes** ◯ **No** ◯ **Unsure**

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. The National Strategy categorizes critical infrastructure as infrastructure that supports any of the following ten sectors:

- *Energy and utilities*
- *Finance*
- *Food*
- *Transportation*
- *Government*
- *Water*
- *Safety*
- *Manufacturing*
- *Information and communication technology*
- *Health*

1.3 Does this research project involve the use of **personal data** that could be sensitive? ◯ **Yes** ◯ **No** ◯ **Unsure**

Personal data includes any information, recorded or not, about an identifiable individual. Personal data can include but is not limited to information relating to the age; culture; disability; education; ethnicity; gender expression and gender identity; immigration and newcomer status; Indigenous identity; language; neurodiversity; parental status/responsibility; place of origin; religion; race; sexual orientation; socio-economic status; blood type; fingerprints; medical, criminal or employment history; financial transactions; and home address.

Personal data should be protected by security measures appropriate to the sensitivity of the information. Some personal data is inherently sensitive (e.g., health and financial data, ethnic and racial origins, political opinions, and genetic and biometric data) and may require a higher degree of protection. The sensitivity of other types of personal information can depend on the context or factors such as how the personal data is used and how much it reveals about an individual. This information will generally be considered sensitive because of the specific risks to individuals when said information is collected, used or disclosed.

*Additional information can be found in **List 2 of Annex A** of the National Security Guidelines for Research Partnerships.*

1.4 Does this research project involve the development or use of **large datasets** that could be sensitive? ◯ **Yes** ◯ **No** ◯ **Unsure**

The sensitivity of a large dataset depends on the nature, type, and state of the information it contains, as well as how it may be used in the aggregate (e.g., in the event that a leak would result in a breach in the privacy of research participants; opportunities for exploitation or coercion; and/or a reputational risk). Large datasets, especially if aggregated, may be analyzed to reveal patterns, trends, and associations, especially related to human behaviour and interactions. Large datasets, if identified as having ethical, commercial, or legal impact on the individual, domestic, or international level could be considered as a lucrative research area with national security considerations.

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)? ◯ **Yes** ◯ **No** ◯ **Unsure**

The ECL defines which goods and technology are controlled for export from Canada to other countries, regardless of their means of delivery. If you are working with items that are included on the ECL as part of this research project, you must answer "yes" to this question, whether or not you plan to export such items to someone outside Canada.

More information on the requirements of the ECL can be found in the Export and Brokering Controls Handbook and in A Guide to Canada's Export Control List. Completing this form does not exempt you from your obligations under the EIPA.

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? ◯ **Yes** ◯ **No** ◯ **Unsure**

This annex provides a list of sensitive research areas that may be updated periodically in accordance with the evolution of technologies, the military and intelligence applications of technology, and national security imperatives. These technologies can be sensitive and are often referred to as "dual-use", meaning that they have military, intelligence, or dual military/civilian applications. Applicants should review this list according to their understanding of any potential applications of their research to assess whether their research may be considered sensitive or dual-use.

Save As | Print | Reset

Section 2: Know Your Partner Organization

The purpose of this section is to assess whether **your partner organization(s)** could pose a national security risk by using the research knowledge, technology and intellectual property resulting from your research project. Your research can be an attractive target for those seeking to steal, use, and adapt it for their own priorities and gains. In some instances, research could lead to advancements in the strategic, military, or intelligence capabilities of other countries or be used to purposefully cause harm to Canada's national security.

The following questions serve as a source of information to assist in determining the overall risk profile of your research partnership. Answering "yes" or "unsure" to any of these questions is not a determinant of a denial of funding.

Answer the following questions to the best of your ability by using information that is already available to you, your institution, or your partner organization(s), or that could be reasonably accessed through open sources. To further support transparency and openness, you are encouraged to consult your partner organization(s) when answering these questions. The Government of Canada may request more information from your partner organization(s) for the purposes of national security risk assessment.

When answering these questions, you must consider and include information not only about your partner organization(s) but also their relevant affiliates. Therefore, for the purpose of this section, the term 'partner organization' also includes any affiliated parent organizations, subsidiaries, and joint ventures in Canada and abroad.

If your research partnership includes several partner organizations, you must complete one Risk Assessment Form that collectively considers the risks associated with all partner organizations.

2.1 Are there any indications that your partner organization(s) could be subject to **foreign government influence, interference or control**? ◯ **Yes** ◯ **No** ◯ **Unsure**

Organizations that are state-owned or subject to state-influence or interference may be a key indicator of non-commercial interest motivations that could facilitate unauthorized knowledge transfer in a manner that could harm Canada's national security (for example, if the research is used for cyber-attacks, military advancement, or surveillance). Some countries have laws or practices that compel entities and individuals to be subject to direction from their governments to provide internationally generated information, research knowledge, technology, and its resulting intellectual property.

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? ◯ **Yes** ◯ **No** ◯ **Unsure**

Indicators of unethical behaviour could include:

- *Individuals associated with your research partner organization(s) that have been charged, admitted guilt or been convicted of fraud, bribery, espionage, or corruption in any jurisdiction.*
- *A partner organization that has been charged, admitted guilt, or convicted of intellectual property, copyright or patent theft in any jurisdiction.*
- *A partner organization that has committed illegal offences related to import or export controls and/or controlled goods.*

An indicator of lack of transparency could include information about unethical behaviour that was not disclosed by your partner organization(s) and that you uncovered by doing your own due diligence searches.

You should focus on events that occurred within the last five years and those that took place prior to the last five years that may have a lasting impact (e.g., an event that has brought the general reputation of the partner organization into disrepute).

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? ◯ **Yes** ◯ **No** ◯ **Unsure**

Risks can originate from personnel from your partner organization(s) that are or will be involved in the project, particularly if individuals have real, perceived, or potential ties to foreign militaries or governments. You are encouraged to work with your partner organization to ensure that all real, perceived, or potential conflicts of interest and affiliations are appropriately disclosed.

Responses to this question should be limited to individuals associated with the partner organization who will contribute and/or have access to your research project, as well as their supervisors, managers and executives.

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**? ◯ **Yes** ◯ **No** ◯ **Unsure**

Access to both physical and digital infrastructure and data could be used to support unauthorized access or knowledge transfer outside the scope of the research partnership. When answering this question consider the access your partner organization(s) may also have to your institution's infrastructure and data for reasons unrelated to this specific project or to any other project(s) they are working on. Examples of potential risks may include a partner organization gaining new access to controlled or restricted areas within a facility, IT systems or networks, specialized equipment or sensitive material that is unrelated to this specific project.

Refer to Questions 1.3 and 1.4 for more information on what constitutes sensitive data.

This question does not include situations where the partner organization(s) already has legitimate access to facilities, networks, or assets on your campus/institution as a result of other partnerships or projects, or where the partner organization(s) would gain access to facilities unrelated to research (e.g., recreational facilities).

Section 3: Risk Identification

The purpose of this section is to collect information on any **risk factors** that you have **identified** in the two first sections of the form. To support the risk assessment process, your response must provide information on the source and nature of the risks.

For each "**yes**" or "**unsure**" response that you provided in the Know Your Research **and** Know Your Partner Organization sections, describe the **resources** you utilized and the **key findings** you gathered.

You may add any other relevant or contextual information related to your partner organization(s) in this section. For example, list any concerns noted during your due diligence process that have not been captured in a previous section of this form.

Maximum of 4,800 characters with spaces.

Section 4: Risk Mitigation Plan

The purpose of this section is to present your **risk mitigation plan**. This plan will ensure that you identify the appropriate mitigation measures to reduce the likelihood of an identified security risk materializing, and/or to lessen the impact in case the identified risk materializes.

When developing your risk mitigation plan, you must address all risk factors that you identified by answering "**yes**" or "**unsure**" to questions in the Know Your Research **and** Know Your Partner Organization sections.

Your risk mitigation plan should be developed **with your institution**. You may also involve your institution's corporate support services (e.g., IT, security, legal) to confirm the viability and feasibility of the proposed measures.

Mitigation measures should be tailored to the research project and commensurate with the risks identified while considering open science principles. For instance, your risk mitigation plan could cover areas, such as, but not limited to:

- Describing any other relevant review processes for which the project has been subject to (e.g., a Research Ethics Board review focusing on how personal data gathered through the research project will be safeguarded)
- Raising research security awareness and building capacity across your research team
- Ensuring that your partner organization(s)' objectives align with the objectives of the partnership
- Ensuring sound cybersecurity and data management practices
- Agreement on the intended use of research findings

For each mitigation measure you propose, you must also provide a **timeline** for its implementation and describe **how you and your institution will monitor its effectiveness**.

It is not sufficient to refer to existing or upcoming policies and practices within your institution. If you refer to a policy or practice, you must also describe **what** this policy or practice entails and **how** it will be applied to mitigate the identified risks.

The National Security Guidelines for Research Partnerships are country and company-agnostic as risks can evolve and originate from anyone and anywhere in the world. Following the principles of the Guidelines, risk mitigation measures must never lead to discrimination against or profiling of a member of the research community. Accordingly, excluding any individual from participating in the proposed research project on the basis of their citizenship or country of residence is **not** an acceptable risk mitigation measure.

Additional information on risk mitigation can be found on the Safeguarding Your Research portal.

Provide your risk mitigation plan in the text box on page 6.

Maximum of 5,400 characters with spaces.

Section 5: Additional Requirements

By submitting this Risk Assessment Form, the applicant on behalf of all co-applicants agrees that, to the best of their knowledge:

- The applicant(s) have not accepted and will not accept any offer of funding that is conditional upon the mirroring of their academic laboratory in, or the transfer of their academic laboratory to, a foreign country; and
- The source of funding and the value of the research project to the partner organization(s) has been communicated by the partner organization(s) to the applicant(s).