NSERC
CRSNG

National Security Guidelines for Research Partnerships

Application to the Alliance program

2021.07.16

Threat actors exploit legal means of knowledge development and collaboration to access research for their own purposes

1. Personnel: individuals who have access to knowledge (insider threats; witting and unwitting participants)
2. Physical Security: access to facilities and physical spaces
3. IT/Cyber: technological access
4. Intellectual Property (IP) and Knowledge: rights, licensing and acquisition
5. Collaboration: partnerships can be used either overtly or covertly

Increased foreign threat to COVID-19 research prompts extraordinary warning from Canada's spy agencies
https://www.cbc.ca/news/politics/cse-csis-china-covid-1.5570134

Canada's chief spy identifies foreign interference and state-sponsored espionage as biggest threat to Canada's prosperity and national interest
https://nationalpost.com/news/canada/significant-and-clear-threat-what-canadas-spy-chief-says-about-china-behind-closed-doors

Iranian hackers selling stolen academic research
https://endpts.com/iranian-hackers-steal-academic-research-worth-billions-from-us-universities-private-companies/

Research Security

To safeguard Canada's research environment from foreign interference, espionage, and unwanted knowledge transfer …

1) The Government of Canada – Universities Working Group (since 2018) has developed **information material** in relation to research security, risks and best practices for researchers (the Safeguarding your Research portal).

2) The Ministers of Innovation, Science and Industry (ISI), of Health, and of Public Safety and Emergency Preparedness (PS) requested (in September 2020) that the agencies undertake a **review of their own processes and policies** (ongoing).

Research Security

The Ministers of ISI, Health, and PS asked (March 24, 2021) that national security considerations be incorporated in the funding decisions of Alliance grants that support research partnerships with private sector organizations

1) Under ISI leadership, The Government of Canada – Universities Working Group was consulted with for the development of **National Security Guidelines for Research Partnerships.**

2) These Guidelines will be applied initially to the NSERC Alliance funding program when private sector organizations are involved in the partnership.

3) All grant applications that have not yet received a decision (as of July 12th) will be asked to fill the Risk assessment form and submit it to NSERC. All new grant applications will nee to be submitted with the Risk assessment form.

NSERC
CRSNG

The Guidelines will initially apply to the NSERC Alliance program…

1) Grant applications will be assessed as per the normal Alliance program merit assessment process and, in addition, NSERC will review the information provided in relation to research security.

2) The funding decision will take into account both the normal Alliance program merit assessment criteria as well as the research security assessment.

3) Where there are security concerns, NSERC will seek advice from relevant National Security Agencies (Public Safety, Canadian Security Intelligence Service, Canadian Centre for Cyber Security, …).

4) The research security assessment will be based on the Risk assessment form submitted by researchers as well as the risk mitigation plan if required.

Research Security

The National Security Guidelines for Research Partnerships will security risks associated with …

I. **The research area and its potential application for military, public safety, intelligence or espionage purposes**

Examples include: Advanced Materials and Manufacturing, Advanced Sensing and Surveillance, Artificial Intelligence, Biotechnology, Energy Generation, Storage and Transmission, Robotics and Autonomous Systems, Energy and Utilities, Information and Communication technology, Advanced Manufacturing.

II. **The Partner organization**

The questions will seek to better understand whether the partner organization is affiliated with governments, militaries, or organizations that could negatively impact Canada's national security, or has been convicted of fraud, bribery, espionage, corruption, or other criminal acts.

Research Security

What will researchers and institutions have to do?

1) Researchers develop a partnership and prepare their application as normal. Researchers also complete the Risk Assessment Questionnaire to help gauge the risks associated with that particular partnership project.

2) Researchers provide the information requested in the Risk Assessment Questionnaire, to the best of their abilities.

3) If risks identified, researchers work with their institution to develop a plan to mitigate those risks.

4) Institutions need to review the risks associated with the proposed partnership prior to the submission of the grant application.

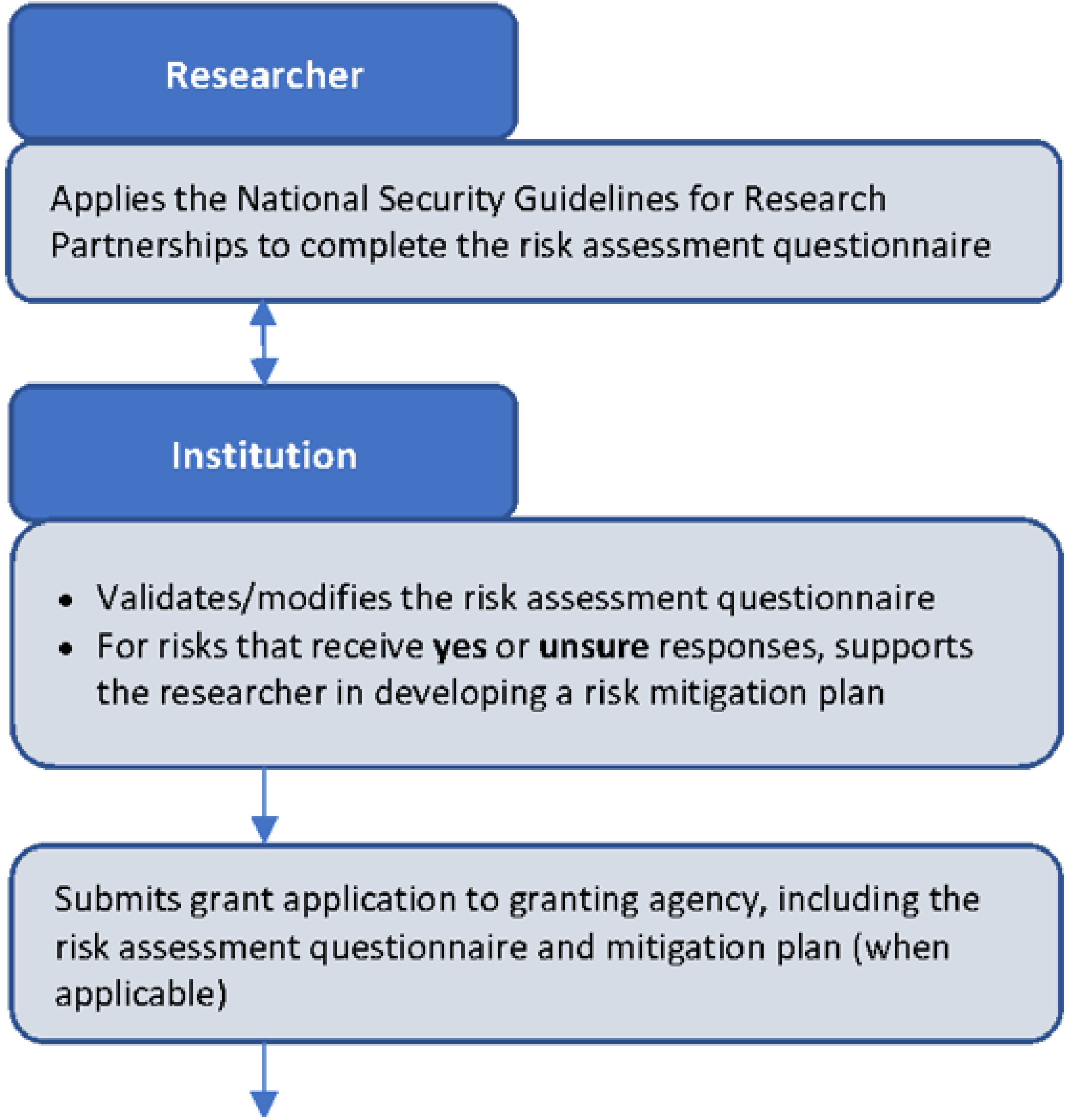
Research Partnerships

Impact of the implementation of the National Security Guidelines for Research Partnerships

- In July 2021, the Government of Canada introduced the National Security Guidelines for Research Partnerships to integrate national security considerations into the development, evaluation, and funding of research partnerships. They were applied immediately to NSERC Alliance grant for applications that include a private sector partner organization.
- NSERC has analyzed key metrics from applications processed through administrative risk validation, after 6 months of the implementation of the Guidelines (July – December 2021).
- Overall, applicants have made a best effort to assess security risks associated with their private sector partner. Most applications do not need advice from national security agencies.

Total applications received for administrative risk validation	**446**		
Applications cleared by NSERC	386	86.5 %	
Applications deemed incomplete	25	5.6 %	Rejected
Applications deemed to not have provided any or sufficient information in relation to the national security questionnaire	11	2.5 %	
Applications referred to a national security agency for advice	24	5.4 %	
Applications where national security agency advice has been received	0		

Assessment process



Researcher

Applies the National Security Guidelines for Research Partnerships to complete the risk assessment questionnaire

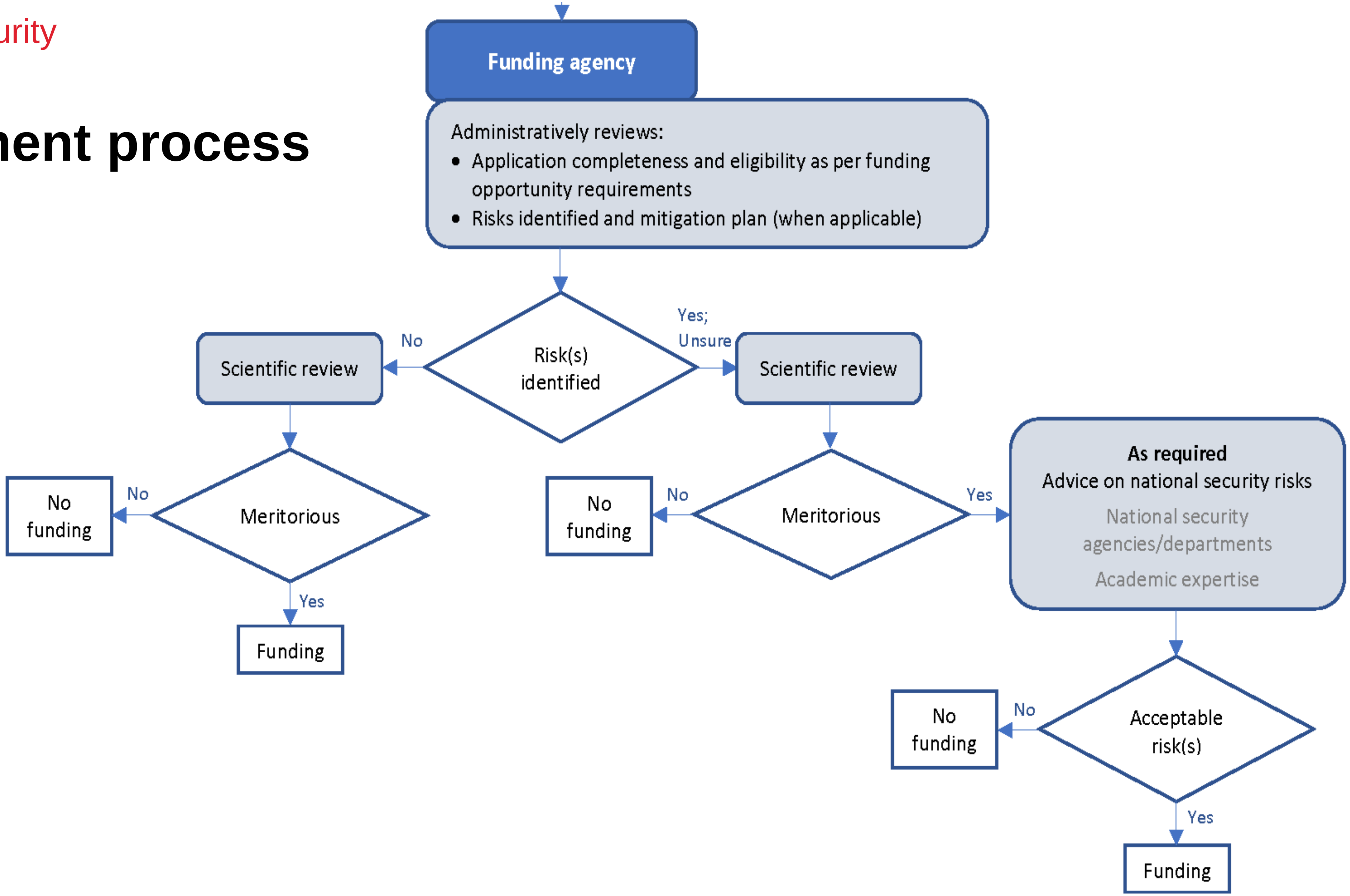
Institution

- Validates/modifies the risk assessment questionnaire
- For risks that receive **yes** or **unsure** responses, supports the researcher in developing a risk mitigation plan

Submits grant application to granting agency, including the risk assessment questionnaire and mitigation plan (when applicable)

Research Security

Assessment process



Funding agency

Administratively reviews:

- Application completeness and eligibility as per funding opportunity requirements
- Risks identified and mitigation plan (when applicable)

As required
Advice on national security risks

National security agencies/departments

Academic expertise

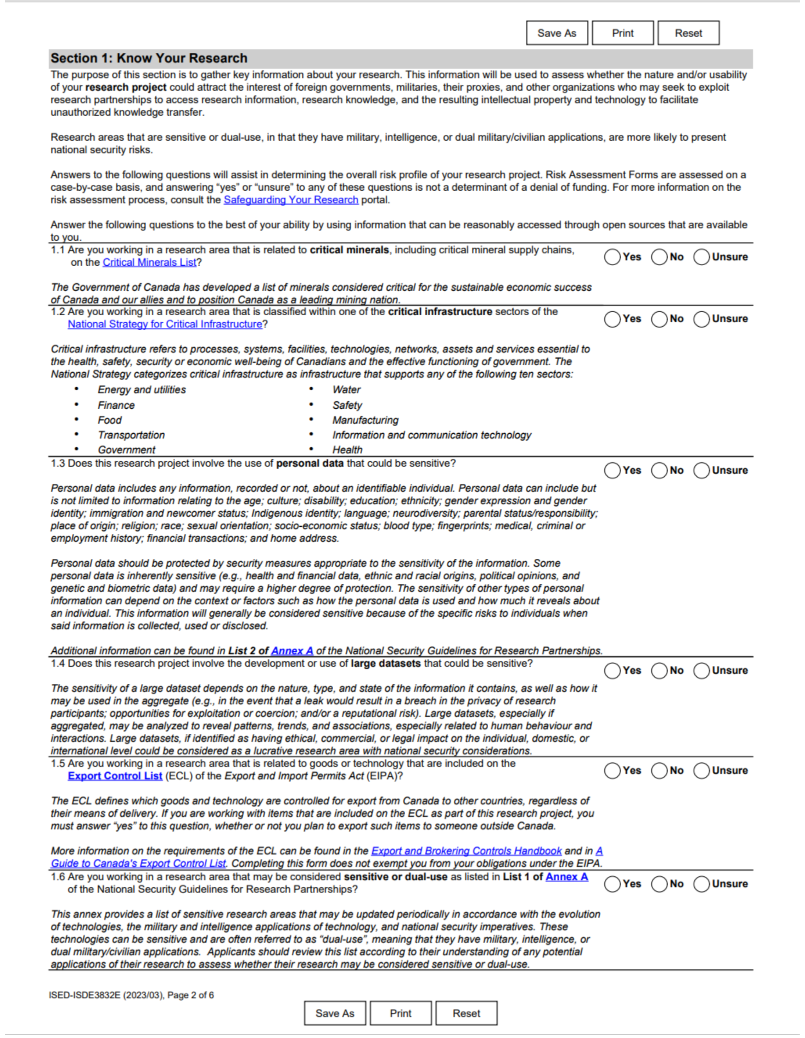
Risk Assessment Form: Review Process

- Step 1:
  - Administrative validation by Agency using open-source due diligence
  - Applications with potential identified risks are referred to Internal Risk Assessment Committee and reviewed. As necessary, some are forwarded to Public Safety Canada

- Step 2:
  - Referral of applications to Public Safety Canada on as-needed basis
    - ie, Canadian Security Intelligence service (CSIS)
  - Decision on which security agency will review
  - Further review by relevant agency

- Step 3:
  - Funding decision

Security Assessment Form: 2023



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**

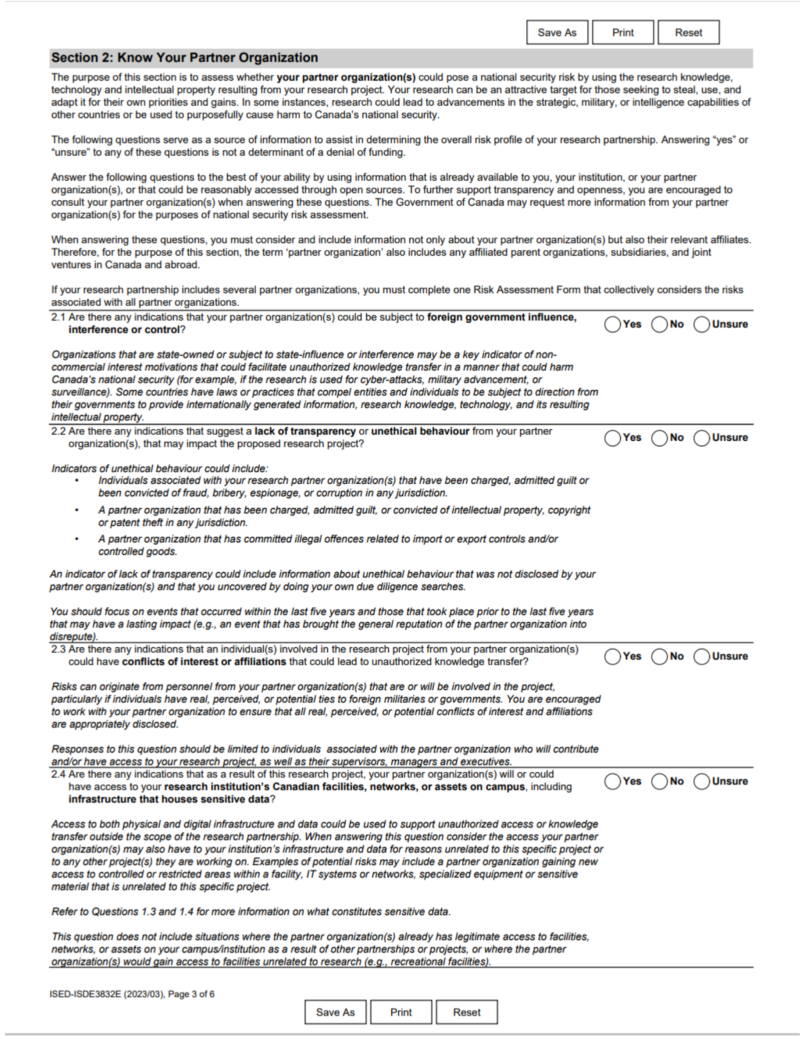
The ECL defines which goods and technology are controlled for export from Canada to other countries, regardless of their means of delivery. If you are working with items that are included on the ECL as part of this research project, you must answer "yes" to this question, whether or not you plan to export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

ISED-ISDE3832E (2023/03), Page 2 of 6



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).

ISED-ISDE3832E (2023/03), Page 3 of 6

Section 1: Know your research

- Critical Minerals
- Critical Infrastructure
  - Energy and utilities, Finance, Food, Transportation, Government, Health Water, Safety, Manufacturing, Information and communication technology
- Personal Data
- Large datasets
- Export Control List
  - If you are working with any of these, regardless of whether you plan on exporting it
- Sensitive or Dual Use: Annex A

Section 2: Know your Partner

- Foreign government influence, interference, or control
- Indications of unethical behaviour
- Conflict of interest or affiliations
- Would the partner have access to facilities, networks, or assets that could house sensitive data

Identify risks: 4,800 characters (with spaces)

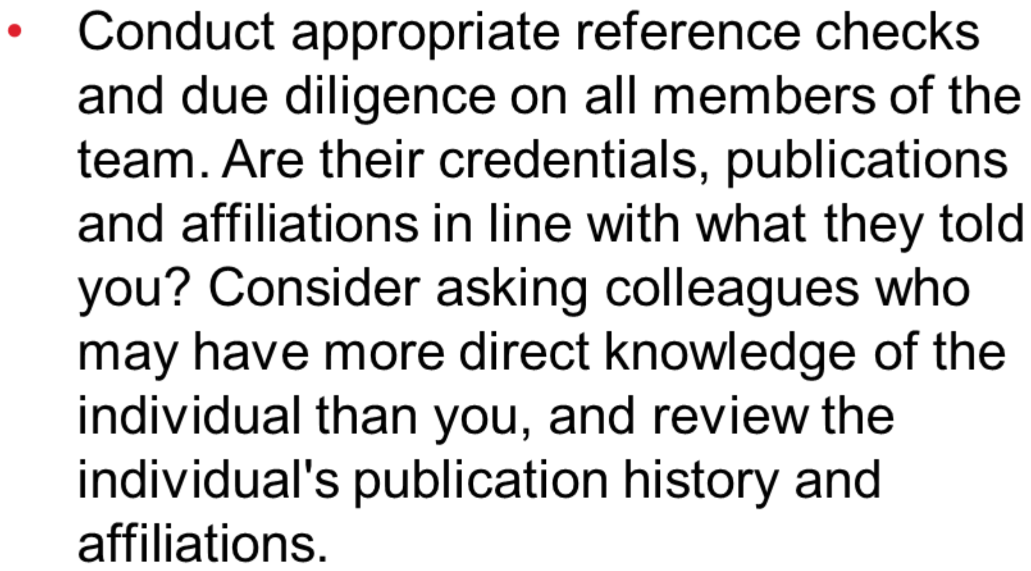
- For any questions where you answered Yes or unsure, identify WHY you answered thusly
  - eg, YES to Critical Infrastructure:
    - "My research focuses on zero-net energy buildings and therefore falls under the category of Energy"
- This box is for both section 1 and 2 risks that you have identified

Risk Mitigation Plan: 5,400 characters (with spaces)

- Should be tailored specifically to your research project
- Address only the risks you have identified
- Resources:
  - Safeguarding your Research
  - Conducting Open-source Due Diligence
  - Safeguarding your research checklist

Building a Strong Research Team:

Verify all team members' professional history and assess alignment with the research priorities for this project.



- Conduct appropriate reference checks and due diligence on all members of the team. Are their credentials, publications and affiliations in line with what they told you? Consider asking colleagues who may have more direct knowledge of the individual than you, and review the individual's publication history and affiliations.

Building a Strong Research Team:

Assess existing or potential conflicts of interest or affiliation that would impede collaboration with any team member.

- Ask yourself, "Could the interests or affiliations of my team members compromise the integrity of my research in a manner that jeopardizes Canada’s national security?"

Building a Strong Research Team:

Discuss project risks internally and make a plan for their mitigation, involving external team members as appropriate.

- Brainstorm potential project security risks with your team.

Assess whether the practices of your collaborator(s) and/or collaborating institution(s) are consistent with your institution's standards on ethics and research conduct.

- Ask yourself whether all aspects of the project, regardless of where the work is or was performed, would pass ethics review at your institution.

Assessing the Alignment of Your Partners Motivations With Your Own:

Ensure the motivations of all partners are clear and aligned with the goals of the research team, including any expectations about intellectual property.

- Ask the partner directly what they expect from the research team during the project and what they hope to get out of the project at the end.

Assessing the Alignment of Your Partners Motivations With Your Own:

Assess if the partner's governance structure is transparent and whether the ultimate beneficiary of their collaboration on your project is clear.

- Looking on the partner's website, can you easily identify who leads the partner organization and any linkages to government, other organizations, and/or other actors? What information gaps exist?

Assessing the Alignment of Your Partners Motivations With Your Own:

Explore if other academics have had positive experiences collaborating with this partner.

- By reaching out to researchers across your institution and at other institutions, you can gather valuable information on past experiences and solutions to address concerns.

Assessing the Alignment of Your Partners Motivations With Your Own:

Assess whether the practices and contributions of your partner(s) are consistent with the standards on ethics and research conduct at your own institution.

- Ask yourself whether any contributions (data, background IP, etc.) are consistent with your institution’s policies and/or Canadian laws.

Ensuring Sound Cybersecurity and Data Management Practices:

Verify that all team members have completed cyber hygiene and data management training.

- Discuss appropriate training options with your CIO or with the relevant resource person in your institution.

Ensuring Sound Cybersecurity and Data Management Practices:

***Assess if the data management and cybersecurity measures needed to adequately protect research integrity are in place across all partners*.**

- Consult your institution's policies and practices and internal research and IT services. Public Safety Canada and the Canadian Centre for Cyber Security offer resources and best practices.

Ensuring Sound Cybersecurity and Data Management Practices:

Focus on addressing divergent cybersecurity and data management practices and decide on a mutually acceptable approach to securing your research data.

- When reflecting on existing divergences, ask yourself, "Given the sensitivity of the research topic and data, what is the level of risk associated with a breach and what is the probability it may occur?"

Ensuring Sound Cybersecurity and Data Management Practices:

If professional or personal international travel is expected during the project, agree to a protocol for device management.

- See the Travel Security Guide for Researchers and Staff for more information.

Agreement on Intended Use of Research Findings:

Agree to a plan of how and when you will share details about the project, including publication, conferences, teaching, mass media, social media and personal communication. This will increase effectiveness and minimize disagreement later.

Assess the potential value of any project- related IP and what you need to do to protect it.

- Ask yourself, "What types of IP could be generated through this research project? What do we need to do to preserve the value of this IP?"

Agreement on Intended Use of Research Findings:

Ensure all collaborators and partners have agreed on how IP will be handled.

- The appropriate contacts at your institution can help you understand your institution's policies with regard to IP, as well as how policies, laws and enforcement might vary across relevant institutions and countries.

Agreement on Intended Use of Research Findings:

Discuss how restrictions on academic freedom or commercial interests may impact the research project and the communication of research results.

- Ask yourself, "Do the restrictions imposed on communicating results have potentially harmful impacts on the integrity of our research or our ability to publish results?"

Agreement on Intended Use of Research Findings:

Ensure all collaborators and partners are comfortable with the likely uses of any research results.

- Brainstorm with your team the likely uses of the results of the project, then ask members if they remain comfortable proceeding with the project.

Agreement on Intended Use of Research Findings:

Ensure mechanisms exist that guarantee that any researcher involved in the project is able to use the results to complete their studies.

- Verify with the appropriate contacts at your institution what measures exist at your institution and make all partners and collaborators aware of this requirement. Participants in NSERC-supported research must ensure that a researcher’s graduation is not impeded by intellectual property issues, and must support the publication of results in the open literature. See the Policy on Intellectual Property for more information.

BUILDING A STRONG RESEARCH TEAM:

- The PI will vet the professional history of all team members (including new hires).
- All research team members will be made aware of all confidentiality obligations in related agreements, and will familiarize themselves with the expectations for research and scholarship integrity as set out in the pertinent NSERC and University policies.
- The PI will require all team members to complete training on research security, cyber security, and intellectual property, such as the relevant workshops, seminars and courses offered by the university's Information and Cyber Security Training and Awareness module.
- Any team member engaging in conference-/project-related travel will be required to review and comply with the University's Off-Campus Activity and Travel Policy, and to register their travel with the University's Off-Campus Travel Registry as required.

ASSESSING ALIGNMENT OF PARTNER ORGANIZATION'S MOTIVATIONS:

- The PI will have regular meetings with the partner organization to evaluate the research progress

ENSURING SOUND CYBERSECURITY AND DATA MANAGEMENT PRACTICES:

- The research team will consult with the university IT personnel in developing and implementing effective strategies for data management and cyber security to handle and store the collected data appropriately considering the national security risks, including but not limited to: (1) removing personally identifying information from research records; (2) establishing a plan and timeline for the retention/disposition of research records in accordance with Tri-Agency research data management policies; (3) limiting data access to credentialed University user accounts; (4) limiting data access to research team members on an "as-needed" basis; and (5) storing all data on password protected servers, cloud, or drives.
- Internal data transmission among team members will be via password-protected servers or drives. Any data files shared with the partner organization will be encrypted, with the password to be shared separately and securely.

AGREEMENT ON INTENDED USE OF RESEARCH FINDINGS:

- An agreement will be undertaken between the applicant's institution and the partner organization. Any IP arising from the research will be subject to the provisions of this agreement and governed by the policies of the applicant's institution and in compliance with Tri-Agency policies.

Advisor, Research Development Contacts

SECTOR	ADVISOR	CONTACT INFORMATION	
Business & Social Sciences	Rebekah Thompson	x 2388	rebekah.thompson@concordia.ca
Engineering & Computer Science	Lauren Segall (BCEE, CME, MIAE) Marjan Shayegan(CSSE, CIISE, CES, ECE)	x4450 x 3263	lauren.segall@concordia.ca marjan.shayegan@concordia.ca
Sciences	Jessica Safarian	x 4465	jessica.safarian@concordia.ca