A Safeguarding Research Overview and How-To

Crafting Successful Risk Assessments and Mitigation Strategies

Nov 2024

REBECCA IRWIN

YORK U

Agenda

This Photo by Unknown Author is licensed under CC BY

Issues Overview & How To (30 Mins)

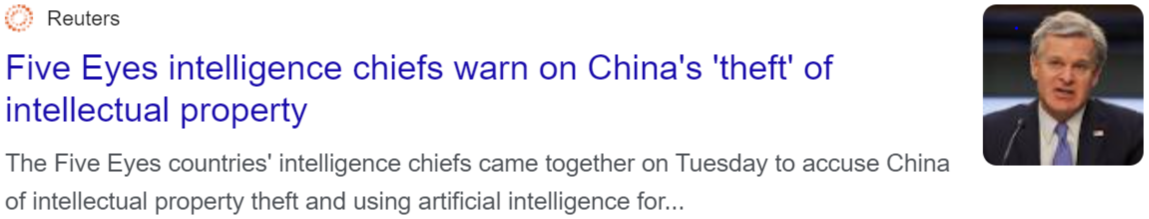
1. Policy Overview
2. Risk Assessment Forms: HOW TO
   I. Sensitive Technology and Research Affiliations of Concern
   II. National Security Guidelines for Research Partnerships
   III. Ontario Research Fund (Mitigating Economic and Geopolitical Risk)

Research Awards Officer Perspective & Best Practices: Soma Tripathi (15 Mins)

PI Perspective: Sunil Bisnath (20 Mins)

Q&A / Discussion (20 Mins)

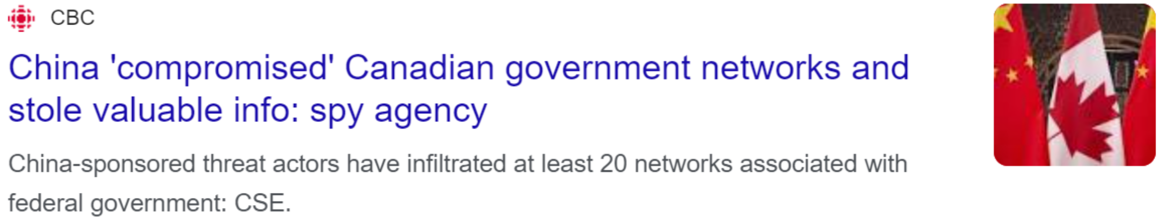
Framing the Issue



Reuters

Five Eyes intelligence chiefs warn on China's 'theft' of intellectual property

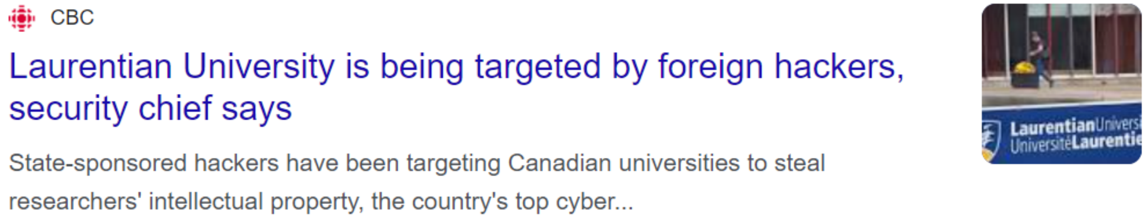
The Five Eyes countries' intelligence chiefs came together on Tuesday to accuse China of intellectual property theft and using artificial intelligence for...



CBC

China 'compromised' Canadian government networks and stole valuable info: spy agency

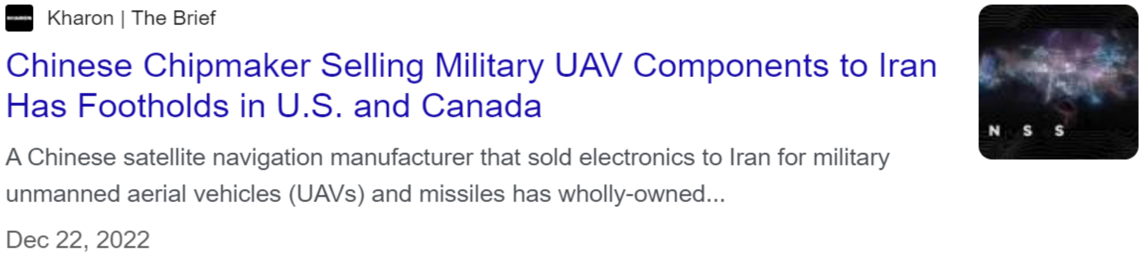
China-sponsored threat actors have infiltrated at least 20 networks associated with federal government: CSE.



CBC

Laurentian University is being targeted by foreign hackers, security chief says

State-sponsored hackers have been targeting Canadian universities to steal researchers' intellectual property, the country's top cyber...

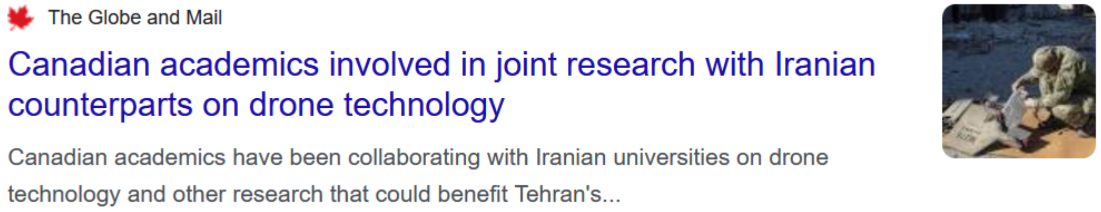


Kharon | The Brief

Chinese Chipmaker Selling Military UAV Components to Iran Has Footholds in U.S. and Canada

A Chinese satellite navigation manufacturer that sold electronics to Iran for military unmanned aerial vehicles (UAVs) and missiles has wholly-owned...

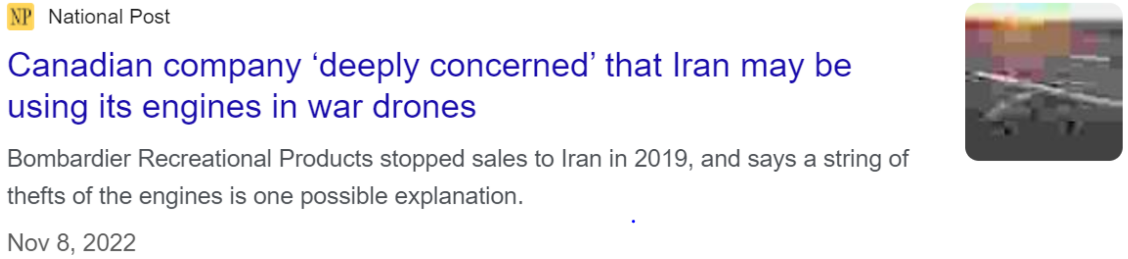
Dec 22, 2022



The Globe and Mail

Canadian academics involved in joint research with Iranian counterparts on drone technology

Canadian academics have been collaborating with Iranian universities on drone technology and other research that could benefit Tehran's...

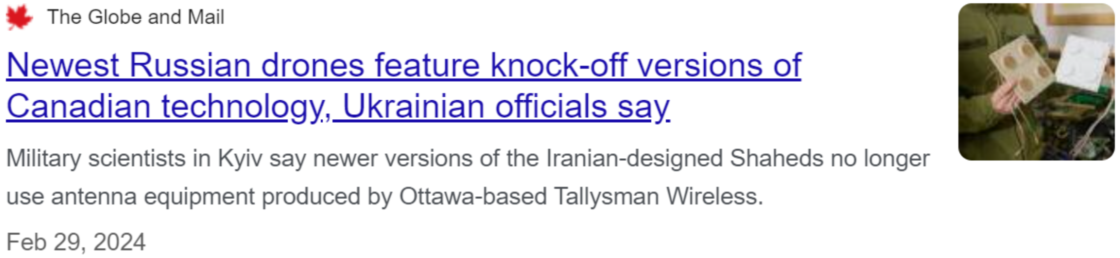


National Post

Canadian company 'deeply concerned' that Iran may be using its engines in war drones

Bombardier Recreational Products stopped sales to Iran in 2019, and says a string of thefts of the engines is one possible explanation.

Nov 8, 2022

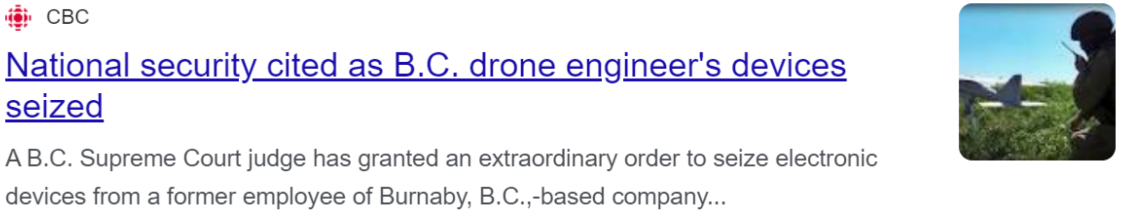


The Globe and Mail

Newest Russian drones feature knock-off versions of Canadian technology, Ukrainian officials say

Military scientists in Kyiv say newer versions of the Iranian-designed Shaheds no longer use antenna equipment produced by Ottawa-based Tallysman Wireless.

Feb 29, 2024



CBC

National security cited as B.C. drone engineer's devices seized

A B.C. Supreme Court judge has granted an extraordinary order to seize electronic devices from a former employee of Burnaby, B.C.,-based company...

Policy Frameworks

Sensitive Technology Research and Affiliations of Concern (STRAC)

National Security Guidelines for Research Partnerships

Ontario Research Fund

Adjacent processes: NRC, Mitacs, etc.

International

**Many policies may impact a project*

Developing Area

Sensitive Technology Research and Affiliations of Concern (STRAC)

Applies to

Canadian Institutes of Health Research (CIHR)

Natural Sciences and Engineering Research Council of Canada (NSERC)

Social Sciences and Humanities Research Council of Canada (SSHRC)

Canada Foundation for Innovation (CFI)

Ontario Research Fund – Implications

Tri-Agency Guidelines

CFI Guidelines

STRAC Lists

List of Sensitive Technology Research Areas STRA

List of Named Research Organizations NRO

Attestation

Those named in a grant proposal that relates to advancing a Sensitive Technology Research area will now sign an attestation regarding that researcher’s current affiliation with an NRO.

Tri-Agency Attestation
CFI Attestation

Compliance

Grant recipients responsible for ensuring that HQP aware of policy, terms & conditions prior to joining team.

Spot checks post award

Intentional omissions subject to recourse based on the Tri-Agency Framework: Responsible Conduct of Research.

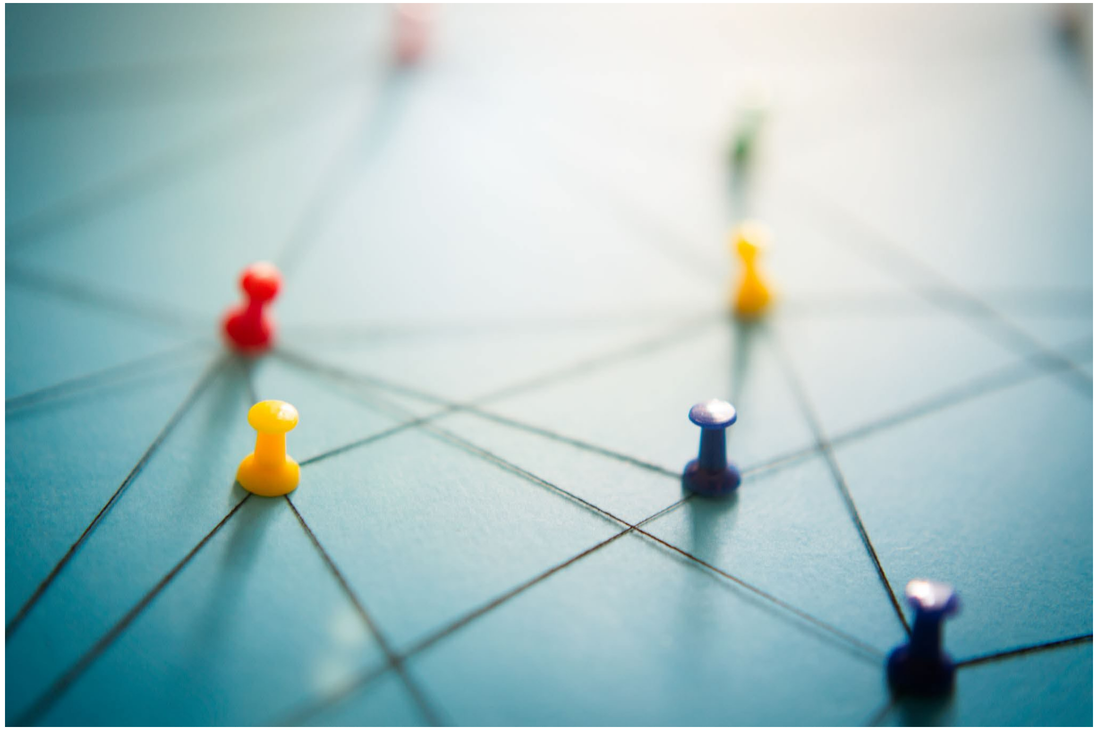
Termination of funding, reimbursement, denial of all future applications, and/or an academic integrity investigation.

References

Policy

FAQ

NATIONAL SECURITY GUIDELINES FOR RESEARCH PARTNERSHIPS (NSGRP)



Assessment of industry partner(s)' associations

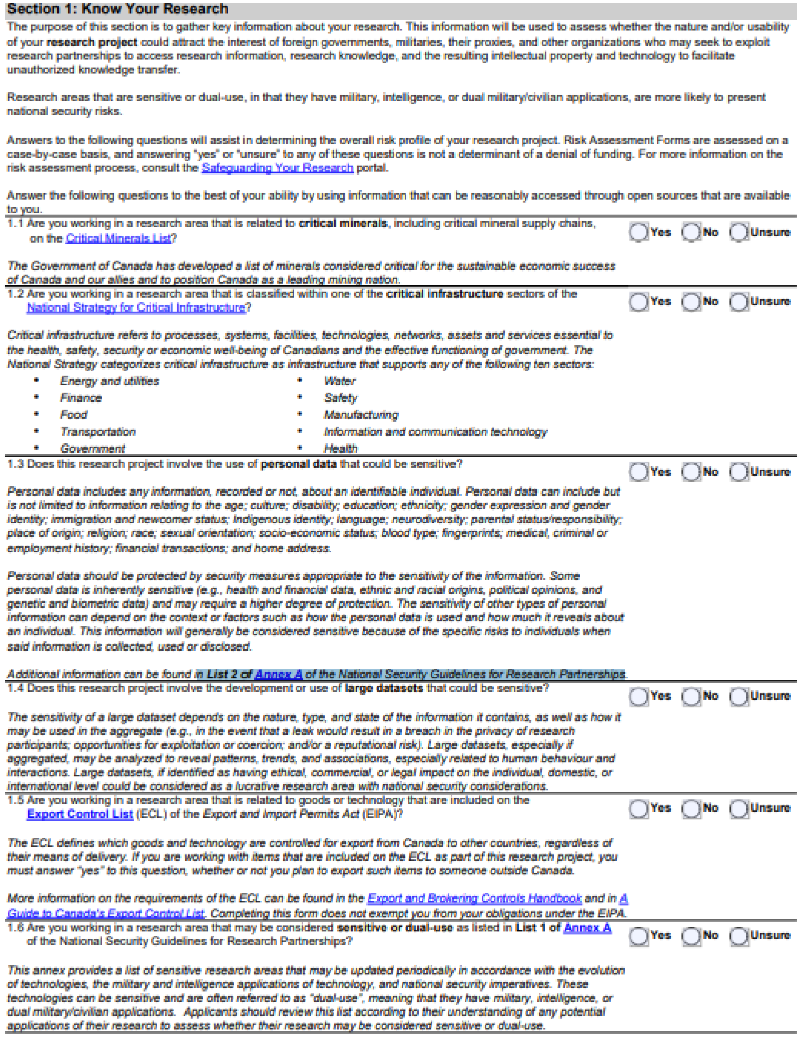
- Risk Assessment Form (RAF)
- NSERC Alliance, CIHR Project Grant, SSHIRC Biomedical Research Fund, CFI

Risks

- Affiliation to military, security
- Mishandling intellectual property / data

Process

How is Risk Assessed
Know Your Research



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

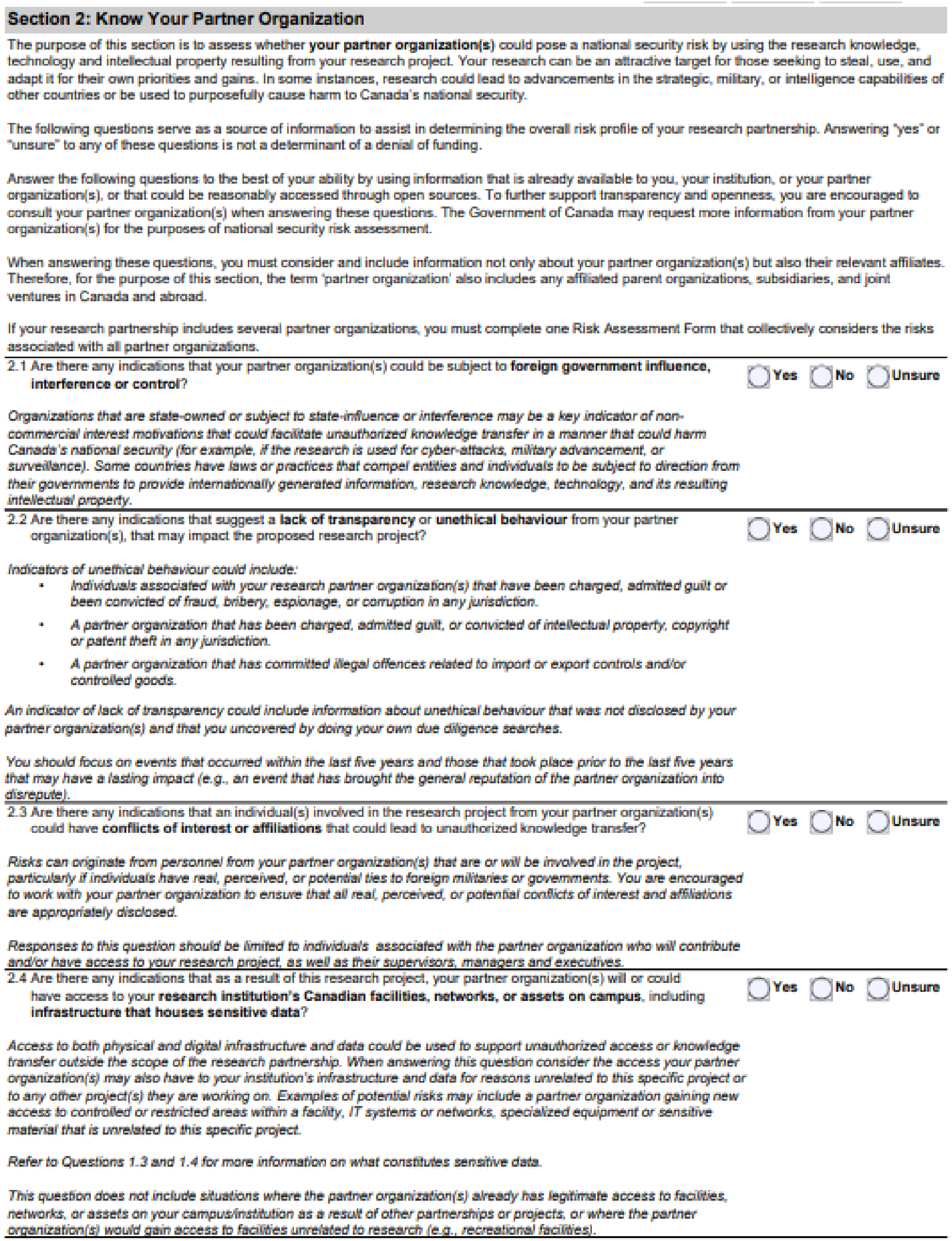
The ECL defines which goods and technology are controlled for export from Canada to other countries, regardless of their means of delivery. If you are working with items that are included on the ECL as part of this research project, you must answer "yes" to this question, whether or not you plan to export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

How is Risk Assessed
Know your Partner



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.

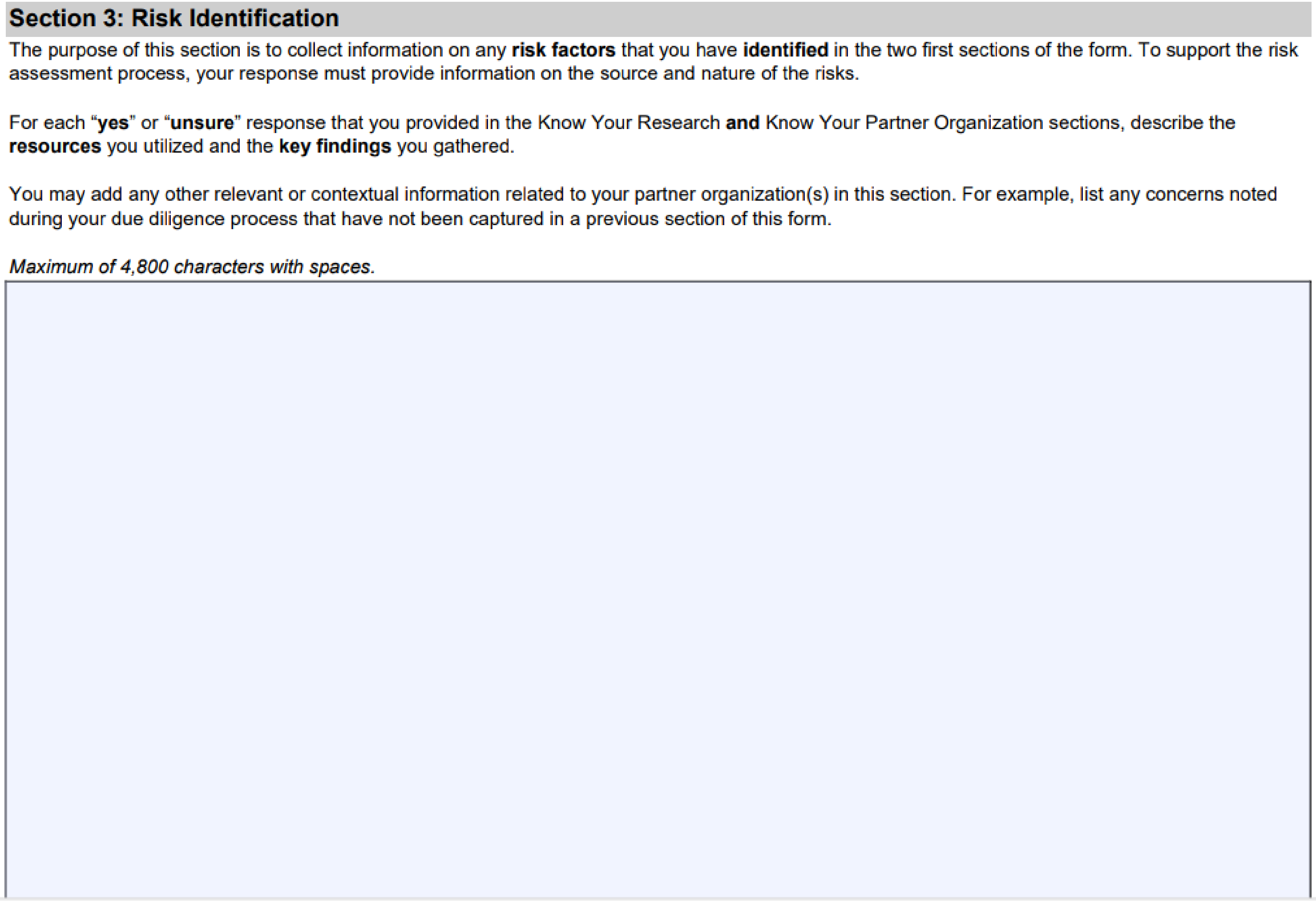
This question does not include situations where the partner organization(s) already has legitimate access to facilities, networks, or assets on your campus/institution as a result of other partnerships or projects, or where the partner organization(s) would gain access to facilities unrelated to research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

(How to) Know Your Partner
Due Diligence

Risk	Tools
Foreign government influence, interference or control	Corporate website, Hoovers, Corporate Registries
Transparency / unethical behaviour such as: fraud, espionage, corruption, IP theft, import / export control evasions	Google news, legal databases (World LII), google, OpenSanctions / Sanctions Explorer (Registering IP elsewhere with clear ties to Canadian research)
Conflicts of interest / affiliation with military or government (researchers, executives)	Press release, google news, IP Databases, Academic Databases (Scopus, Dimensions, etc.)
Operates in geographic areas where data and IP is vulnerable	News, Corporate website
RESOURCE: Conducting Open Source Due Diligence for Safeguarding Research Partnerships	

‘Partner organization’ also includes any affiliated parent organizations, subsidiaries, and joint ventures in Canada and abroad.

Risk Assessment



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.

Risk Mitigation Plans

Note: Must implement
Resource: What steps can you take to protect your research?

Build a Strong Project Team

- Agreement on research use
- Collaboration history
- Conflicts of interest

Non-Academic Partners

- Motivations aligned
- Governance
- Reputation risk
- History of collaboration

Cyber Security

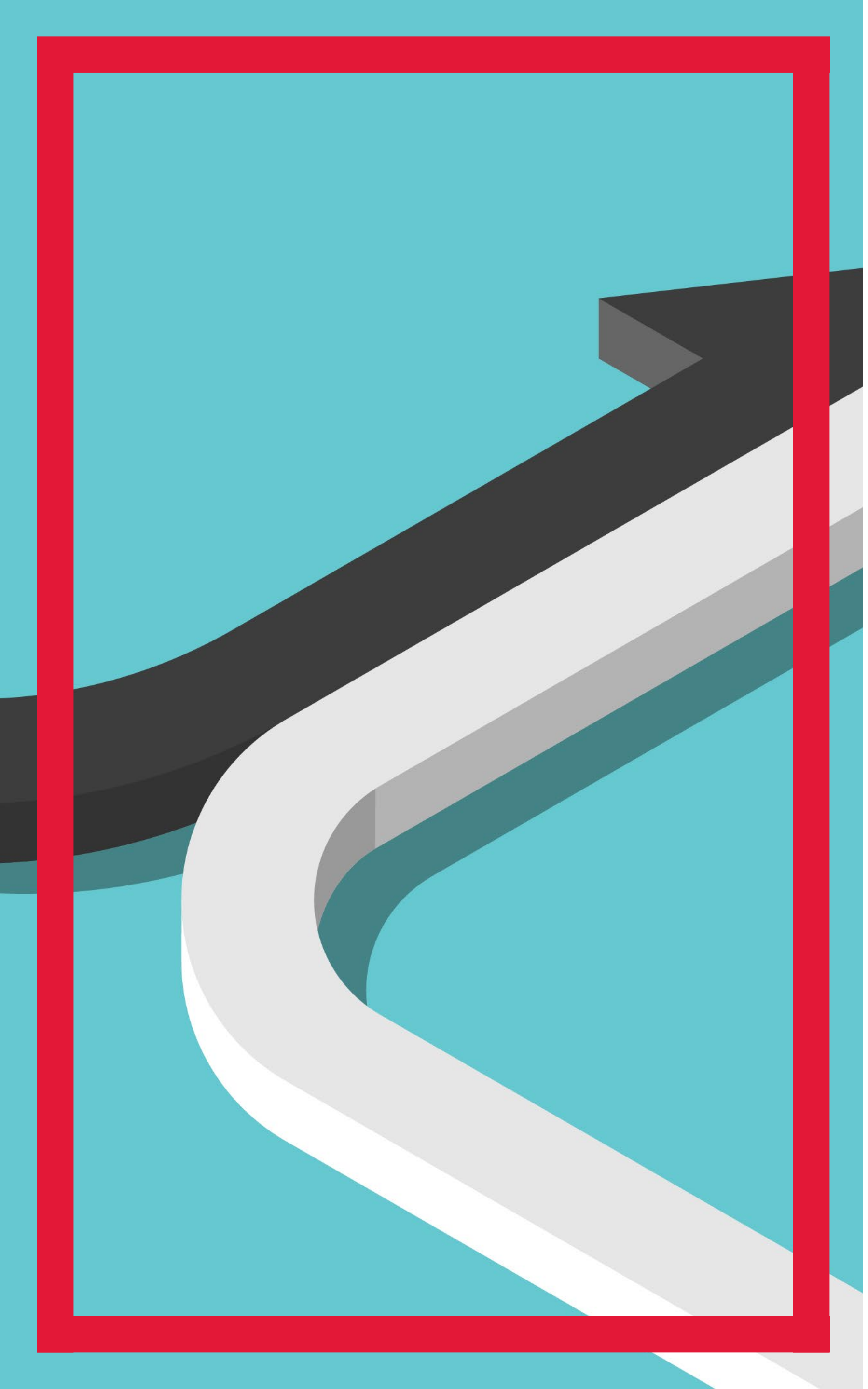
- Data management / security measures
- Training
- Mutually Accepted Approach

Use of Research Findings

- How, What and When public
- **Value of IP and how to Protect**
- Commercial impact
- Grad students use

International Travel

- Risks to persons
- Cyber hygiene



ONTARIO RESEARCH FUND

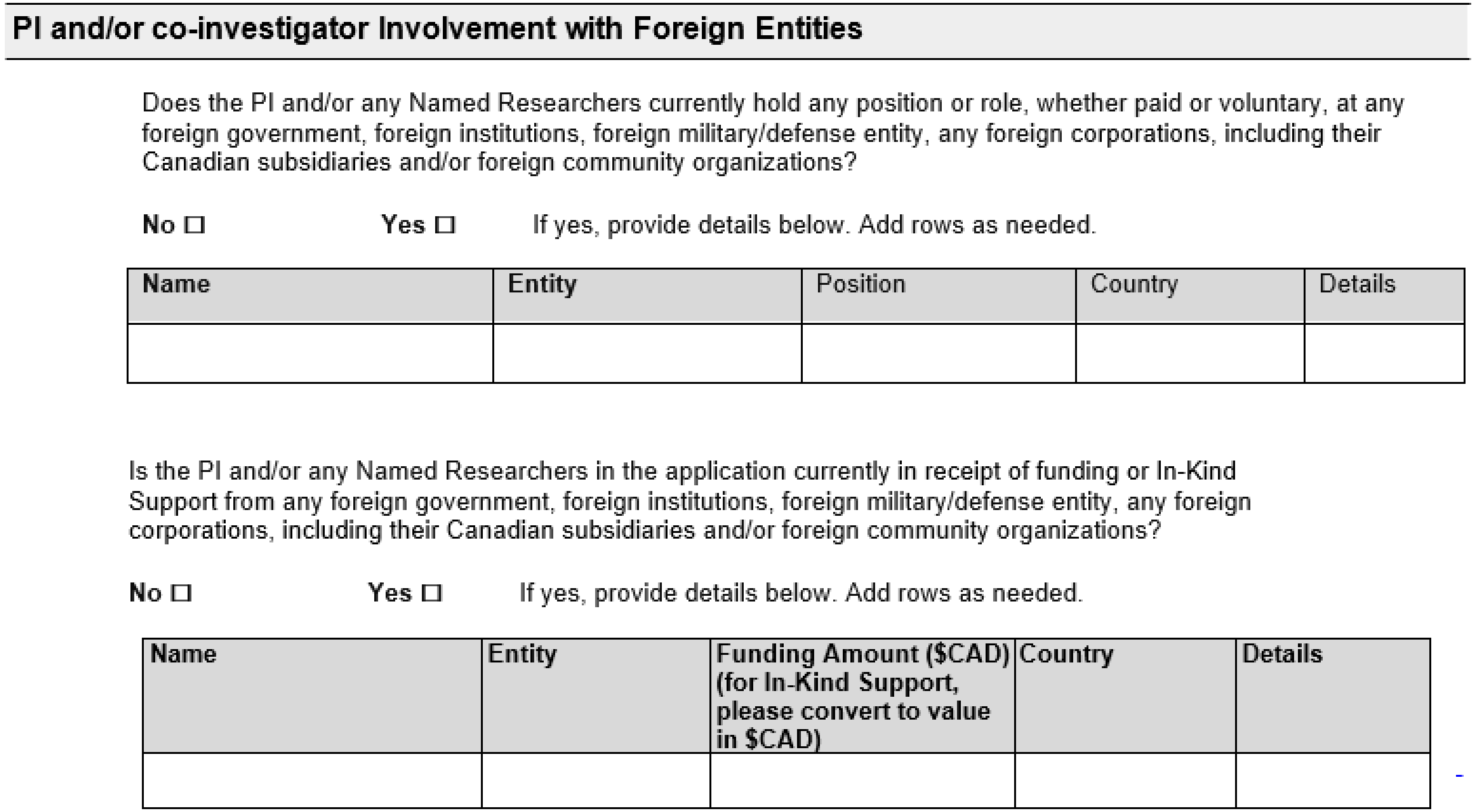
1. Attestation process
Affiliation with Named Research Organization

2. Mitigating Economic & Geopolitical Risk Form
In sensitive research areas, Ontario conducts open-source due diligence checks on all project partners covering previous two years to identify association to entities of concern (beyond NRO).

a. Mitigating Economic and Geopolitical Risk Checklist (updated)
b. Research Security Guidelines and FAQs (new)

Process

Ontario Mitigating Economic and Geopolitical Risk Declaration



PI and/or co-investigator Involvement with Foreign Entities

Does the PI and/or any Named Researchers currently hold any position or role, whether paid or voluntary, at any foreign government, foreign institutions, foreign military/defense entity, any foreign corporations, including their Canadian subsidiaries and/or foreign community organizations?

No □ **Yes** □ If yes, provide details below. Add rows as needed.

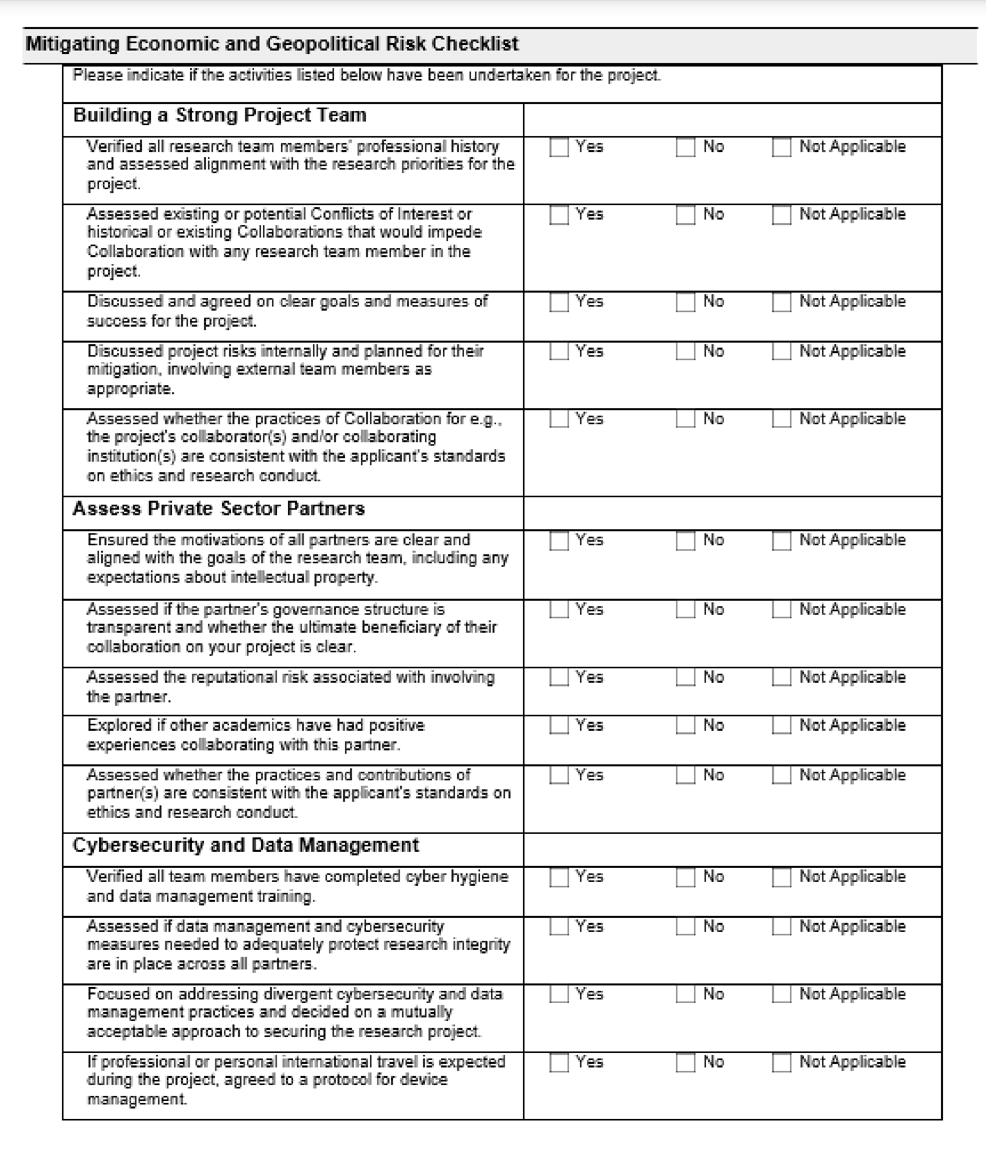
Name	Entity	Position	Country	Details

Is the PI and/or any Named Researchers in the application currently in receipt of funding or In-Kind Support from any foreign government, foreign institutions, foreign military/defense entity, any foreign corporations, including their Canadian subsidiaries and/or foreign community organizations?

No □ **Yes** □ If yes, provide details below. Add rows as needed.

Name	Entity	Funding Amount ($CAD) (for In-Kind Support, please convert to value in $CAD)	Country	Details

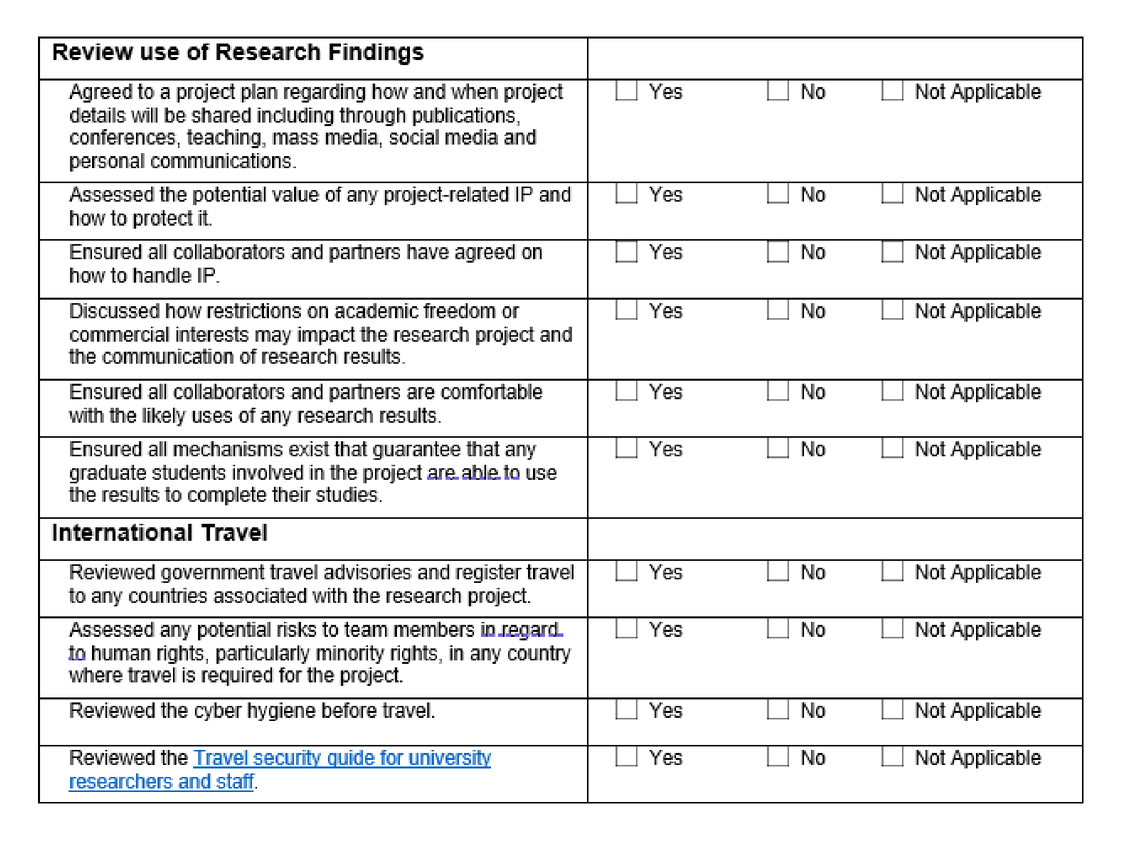
Ontario Mitigating Economic and Geopolitical Risk Checklist



Mitigating Economic and Geopolitical Risk Checklist

Please indicate if the activities listed below have been undertaken for the project.

Building a Strong Project Team			
Verified all research team members' professional history and assessed alignment with the research priorities for the project.	□ Yes	□ No	□ Not Applicable
Assessed existing or potential Conflicts of Interest or historical or existing Collaborations that would impede Collaboration with any research team member in the project.	□ Yes	□ No	□ Not Applicable
Discussed and agreed on clear goals and measures of success for the project.	□ Yes	□ No	□ Not Applicable
Discussed project risks internally and planned for their mitigation, involving external team members as appropriate.	□ Yes	□ No	□ Not Applicable
Assessed whether the practices of Collaboration for e.g., the project's collaborator(s) and/or collaborating institution(s) are consistent with the applicant's standards on ethics and research conduct.	□ Yes	□ No	□ Not Applicable
Assess Private Sector Partners			
Ensured the motivations of all partners are clear and aligned with the goals of the research team, including any expectations about intellectual property.	□ Yes	□ No	□ Not Applicable
Assessed if the partner's governance structure is transparent and whether the ultimate beneficiary of their collaboration on your project is clear.	□ Yes	□ No	□ Not Applicable
Assessed the reputational risk associated with involving the partner.	□ Yes	□ No	□ Not Applicable
Explored if other academics have had positive experiences collaborating with this partner.	□ Yes	□ No	□ Not Applicable
Assessed whether the practices and contributions of partner(s) are consistent with the applicant's standards on ethics and research conduct.	□ Yes	□ No	□ Not Applicable
Cybersecurity and Data Management			
Verified all team members have completed cyber hygiene and data management training.	□ Yes	□ No	□ Not Applicable
Assessed if data management and cybersecurity measures needed to adequately protect research integrity are in place across all partners.	□ Yes	□ No	□ Not Applicable
Focused on addressing divergent cybersecurity and data management practices and decided on a mutually acceptable approach to securing the research project.	□ Yes	□ No	□ Not Applicable
If professional or personal international travel is expected during the project, agreed to a protocol for device management.	□ Yes	□ No	□ Not Applicable



Review use of Research Findings			
Agreed to a project plan regarding how and when project details will be shared including through publications, conferences, teaching, mass media, social media and personal communications.	□ Yes	□ No	□ Not Applicable
Assessed the potential value of any project-related IP and how to protect it.	□ Yes	□ No	□ Not Applicable
Ensured all collaborators and partners have agreed on how to handle IP.	□ Yes	□ No	□ Not Applicable
Discussed how restrictions on academic freedom or commercial interests may impact the research project and the communication of research results.	□ Yes	□ No	□ Not Applicable
Ensured all collaborators and partners are comfortable with the likely uses of any research results.	□ Yes	□ No	□ Not Applicable
Ensured all mechanisms exist that guarantee that any graduate students involved in the project are able to use the results to complete their studies.	□ Yes	□ No	□ Not Applicable
International Travel			
Reviewed government travel advisories and register travel to any countries associated with the research project.	□ Yes	□ No	□ Not Applicable
Assessed any potential risks to team members in regard to human rights, particularly minority rights, in any country where travel is required for the project.	□ Yes	□ No	□ Not Applicable
Reviewed the cyber hygiene before travel.	□ Yes	□ No	□ Not Applicable
Reviewed the Travel security guide for university researchers and staff.	□ Yes	□ No	□ Not Applicable

Ontario Mitigating Economic and Geopolitical Risk Text Box

1. Declare / Detail “Risky” “Collaborations”: 2 Years prior – Project Completion

- Named Research Organizations
- Home – Chinese Defence Universities Tracker — ASPI (Very High, High, Med)
- US DoD List
- Sanctions

2. Know your Research

- Is your research considered “sensitive” (See NSGRP form)

3. Detail how risk assessed / mitigated using these headers

- Building a strong project team
- Non-Academic Partners
- Cybersecurity & Data Management
- Use of Research Findings
- International Travel

Must implement

MCU Definitions

- **Conflicts of Interest (CoI)**: May occur when Funding Beneficiaries have **undeclared appointments, roles, and any material relationship** with a foreign entity.

- **Conflicts of Commitment (CoC):** May occur when a principal investigator's (PI's) time becomes committed to two different activities or to the **same activity that is funded by two different sources**.

- **Collaboration:** Scientific collaboration including but not limited to collaborations involving **co-authorship, co-publication, co-hosting of international conferences, joint research, or joint funding recipients**. This may also include more formal relationships such as a memorandum of understanding, **partnership, joint venture, joint funding, joint degree/exchange program, graduate student supervision, visiting scholar, or participation in a foreign funded talent program**.

MCU Definitions (Con't)

- **Funding Beneficiaries**: Any individual identified in the Ministry research funding program application who would be a partial beneficiary of the funding, primarily: **PI, other researchers on the research team (co-investigators), industry and commercial partners, visiting scholars, students and staff** who may also potentially become Highly Qualified Personnels (HQPs).

- **In-Kind Support**: Non-cash contributions in the form of a **good or a service donation** received by the PI or any co-investigator(s). Examples may include, but are not limited to; **lab equipment, consultation, travelling tickets, and hotel accommodations.**

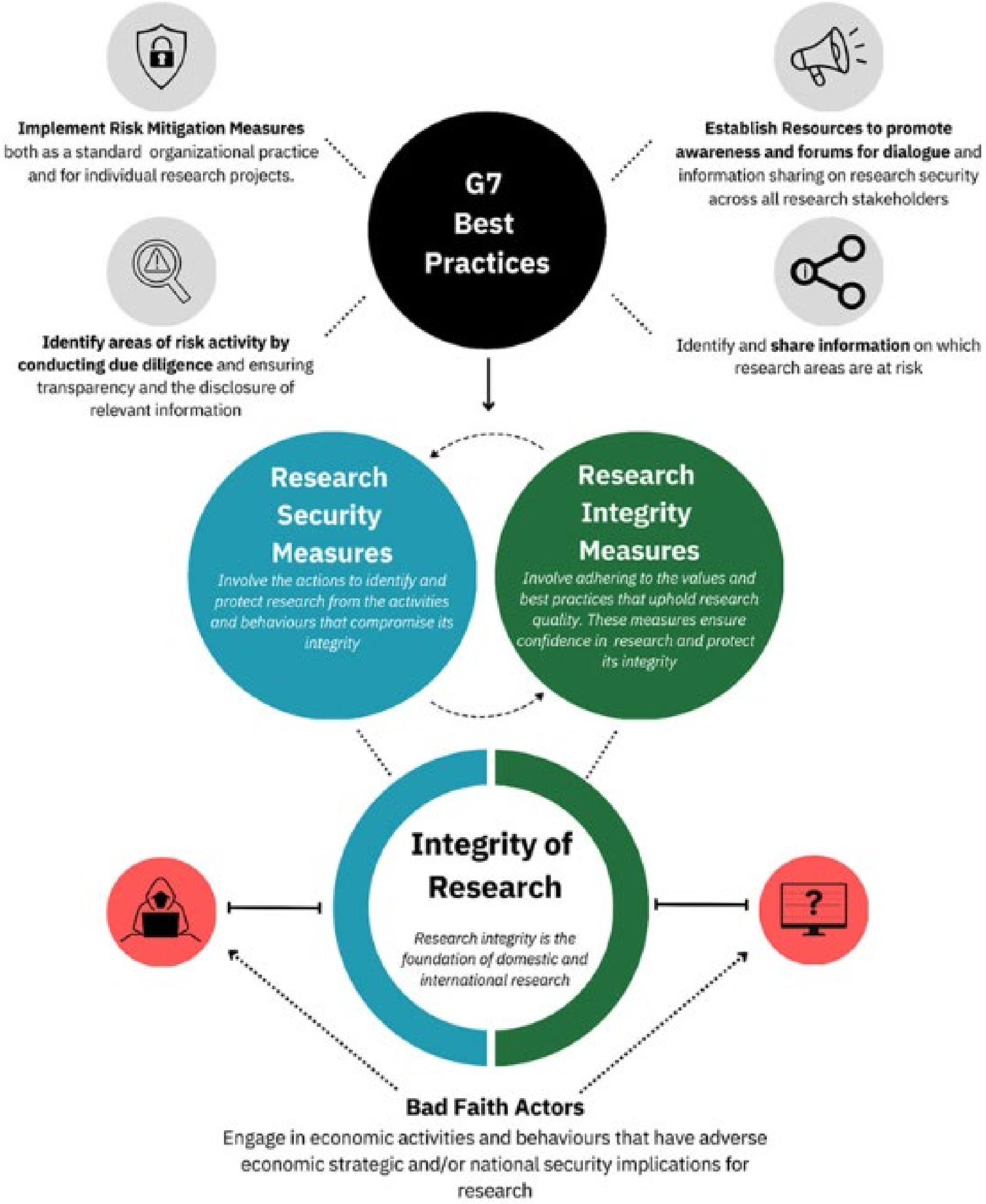
- **Non-disclosure:** When Collaborations, relationships involving funding or In-Kind Support, Conflicts of Interest and/or Conflicts of Commitment are not disclosed in the application as required and the due diligence uncovered material evidence to support the existence of any of the foregoing.

- **Relevant Period**: for the purposes of research security evaluation including the Application Attestation Form, the relevant period encompasses **two (2) years prior to the date the Named Researcher signs the Application Attestation Form through to the anticipated completion date of the proposed project.**

Issues

Open Science

The continuation of a collaborative research system where the importance of all talent – domestic and international – is acknowledged. Openness and security are not contradictory but complementary and mutually reinforcing. G7



G7 Best Practices

Implement Risk Mitigation Measures both as a standard organizational practice and for individual research projects.

Establish Resources to promote awareness and forums for dialogue and information sharing on research security across all research stakeholders

Identify areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information

Identify and **share information** on which research areas are at risk

Research Security Measures

Involve the actions to identify and protect research from the activities and behaviours that compromise its integrity

Research Integrity Measures

Involve adhering to the values and best practices that uphold research quality. These measures ensure confidence in research and protect its integrity

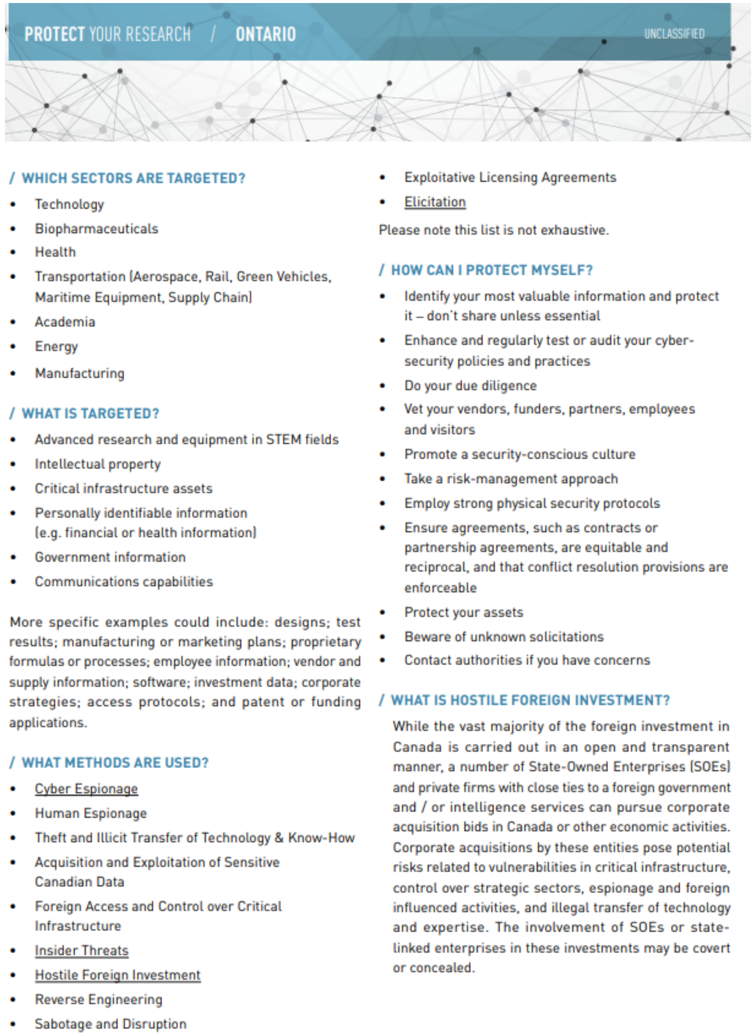
Integrity of Research

Research integrity is the foundation of domestic and international research

Bad Faith Actors

Engage in economic activities and behaviours that have adverse economic strategic and/or national security implications for research

Intellectual Property Protections



PROTECT YOUR RESEARCH / ONTARIO

UNCLASSIFIED

/ WHICH SECTORS ARE TARGETED?

- Technology
- Biopharmaceuticals
- Health
- Transportation (Aerospace, Rail, Green Vehicles, Maritime Equipment, Supply Chain)
- Academia
- Energy
- Manufacturing

/ WHAT IS TARGETED?

- Advanced research and equipment in STEM fields
- Intellectual property
- Critical infrastructure assets
- Personally identifiable information (e.g. financial or health information)
- Government information
- Communications capabilities

More specific examples could include: designs; test results; manufacturing or marketing plans; proprietary formulas or processes; employee information; vendor and supply information; software; investment data; corporate strategies; access protocols; and patent or funding applications.

/ WHAT METHODS ARE USED?

- Cyber Espionage
- Human Espionage
- Theft and Illicit Transfer of Technology & Know-How
- Acquisition and Exploitation of Sensitive Canadian Data
- Foreign Access and Control over Critical Infrastructure
- Insider Threats
- Hostile Foreign Investment
- Reverse Engineering
- Sabotage and Disruption
- Exploitative Licensing Agreements
- Elicitation

Please note this list is not exhaustive.

/ HOW CAN I PROTECT MYSELF?

- Identify your most valuable information and protect it – don't share unless essential
- Enhance and regularly test or audit your cyber-security policies and practices
- Do your due diligence
- Vet your vendors, funders, partners, employees and visitors
- Promote a security-conscious culture
- Take a risk-management approach
- Employ strong physical security protocols
- Ensure agreements, such as contracts or partnership agreements, are equitable and reciprocal, and that conflict resolution provisions are enforceable
- Protect your assets
- Beware of unknown solicitations
- Contact authorities if you have concerns

/ WHAT IS HOSTILE FOREIGN INVESTMENT?

While the vast majority of the foreign investment in Canada is carried out in an open and transparent manner, a number of State-Owned Enterprises (SOEs) and private firms with close ties to a foreign government and / or intelligence services can pursue corporate acquisition bids in Canada or other economic activities. Corporate acquisitions by these entities pose potential risks related to vulnerabilities in critical infrastructure, control over strategic sectors, espionage and foreign influenced activities, and illegal transfer of technology and expertise. The involvement of SOEs or state-linked enterprises in these investments may be covert or concealed.

Know your Partner

Protect your IP

[Safeguarding Research - Research & Innovation (yorku.ca)]

Rebecca Irwin
Director
rirwin1@yorku.ca