June 2026

Guidance on Completing the Ontario Mitigating Economic and Geopolitical Risk Checklist and Attestation Forms

Note: This tool is intended for your use only. **Do not submit this** as part of your grant application package.

The Mitigating Economic and Geopolitical Risk Checklist assists applicants in conducting a risk assessment of their project to identify and address potential economic and geopolitical risks. One checklist is required per application, regardless of the number of participants and your answer selections in the Application Attestation form.

Part 1: Mitigating Economic and Geopolitical Risk Checklist

For each checklist question if you select “no” or “not applicable” please address the reasoning in the text-based “Potential Risk Identified and Risk Mitigation Proposal” section.

Part 2: Potential Risk Identified and Risk Mitigation Proposal

This text-based section allows the PI to contextualize any identified risks and establish mitigation strategies. Do not ignore the above, even if the risk seems minimal to none. Explain as such, and include your reasoning as to why.

Potential Risk Identified

What to consider: If any Named Researchers, including the PI, has indicated they maintain a collaboration or are in receipt of funding or in-kind support from a foreign entity, the PI must address the related risks and set out mitigation measures.

Particularly focus on providing information about collaborations (including co- publications/co-authorships) with entities that could pose an elevated security risk. This includes but is not limited to:

- Institutions on the Government of Canada’s (GoC’s) Named Research Organizations list
- Entities on the United States Department of Defense’s List of Foreign Institutions Engaging in Problematic Activities to Counter Unauthorized Technology Transfer
- Corporations that have been sanctioned by NATO countries. (e.g. the Canadian Sanctions List, the EU Sanctions Tracker, the US Office of Foreign Assets Control List, the US Bureau of Industry and Security Entity List) and the US Consolidated Screening List
- Foreign government research institutions or labs

In addition, the PI and/or Named Researchers should disclose any current or past participation in talent programs administered or funded by a foreign government or entity, regardless of when the participation occurred.

Report an international research collaboration or industrial partnership if you are in doubt as to whether it could be considered an elevated risk.

MCURE's review process prioritizes risks to research via collaborations. Applicants must disclose collaborations with entities that could be considered to pose an elevated security risk.

Collaborations include:

- Currently holding any position or role, whether paid or voluntary
- Receiving funding or in-kind support
- Co-publishing
- Industry partnerships and collaborations
- Graduate student supervision
- Participation as or research with a visiting scholar

Developing a Risk Mitigation Proposal

MCURE expects the risk mitigation proposal to contain an explanation of all identified collaborations as well as mitigation strategies to ensure the safety of the proposed research.

Discuss the following in your response, as applicable:

- Explanations of the collaboration should address items such as was it:
  - Via a former student/post doc who is no longer with Brock?
  - Via a 3rd party researcher?
  - A public lecture or conference?
  - A deep partnership? If so, what is the nature of the partnership?
- When did the collaboration start?
- Was foreign funding involved?
- Are there yet-to-be published papers from this collaboration?
- Were patents or intellectual properties created?
- Is the collaboration ongoing or finished?

Examples of risk mitigation categories under which the PI may consider proposing specific tactics include:

- Training (I.e. Research security, cyber security and intellectual property training)
- Guidance and best practices
  - Government of Ontario's Research Security Guidelines for Ontario Research Funding Programs
  - GoC's Guidelines and Tools to Implement Research Security
- Partnership agreements that include intellectual property and technology transfer clauses that address national security risks
- Data management and Information Security
  - Brock's Cyber Security Awareness and Training
- Establishing access restrictions for partners and personnel to an "as needed" basis
- Reporting mechanisms to your institution on the implementation and effectiveness of the proposed risk mitigation measures

General Points

Have a Data Management Plan (DMP) developed for your lab; ensure lab members have completed relevant cyber security training, and cyber hygiene for international travel training/reading; know who has access to your lab, including adjacent colleagues and their HQP; understand you past collaborations in terms of international institutions and organizations.

These general points will help make completing this form easier. We must show that you have taken this form seriously and completed it to the best of your understanding/knowledge.

Assistance

For assistance completing the forms referenced in this document, please contact Brock's Office of Research Services (ORS).

For general assistance in navigating the Ontario funding process please visit the Research at Brock webpage and visit Brock's Safeguarding your research webpage.

Note: Q: When do researchers need to select Option B in the Application Attestation? A: When a collaboration with an NRO occurred, or the researcher is in receipt of funding or in-kind support from an NRO, during the relevant period.