# Safeguarding Your Research Checklist

**These are some questions to consider. Together, the answers to these questions can help you to assess your level of risk and will inform possible mitigation strategies.**

1. Ask yourself: How might an adverse foreign interest exploit your research or product?
2. Ask yourself: How might an adverse foreign interest exploit "usual" requests for cooperation, access or sharing?
3. Are you aware of specific and/or suspicious foreign interest in your research or product?
4. Have you had any requests for visits to your facilities from foreign delegations? If such a visit transpired, were there any unusual requests or any breaches of security practices during the visit? Did anyone attempt to extract or engage with your network during the visit (e.g., inserting a USB stick or taking photographs)?
5. Have foreign researchers expressed an unusual interest in obtaining the details of your research/product?
6. Do you actively monitor and audit the computer usage of your employees?
7. Have you considered customizing computer access or removable media use for certain groups of employees or physical work areas?
8. Do you have processes and policies in place to monitor your networks and detect large data exfiltrations?
9. Have you had any offers from foreign entities to purchase or invest in your research/product? If so, from whom and what were the terms of the offer? Where those terms unusually generous, confident, or with less due diligence than you might have expected?
10. What is the source of your current funding?
11. Do you control access to specific technologies or know-how on a need-to-know basis?
12. Do you have up-to-date and enforceable conflict-of-interest policies?
13. Do you have a process in place to determine whether your employees are engaged in work or research activities beyond your organisation, while working for you? (e.g. universities, other companies, etc.)
14. Do you know who owns the patents related to your work?
15. Does your research/product have multiple uses? Can you imagine a scenario in which your research/product could be used for malicious purposes regardless of intended use? Is your research strategic/novel/ground-breaking or could it otherwise fill in an important piece of the puzzle for a competitor?

16. Have you or anyone you know (friends/family/colleagues) ever been employed/ offered employment or invited to visit a foreign research facility that conducts similar research or creates similar products?

17. Do you have an employee travel policy or a videoconference policy to ensure your awareness of what is being shared with foreign entities?

18. If anyone from your organisation travelled to a country that exhibits adversarial behaviour towards Canada, did they bring any electronic devices? Were they checked before and after for any signs of compromise? Do you use dedicated devices for international travel?

19. What is the vetting process for hiring foreign researchers at your facility? (This may include students, professors, contractors, etc.)

20. Are you aware of any compromises or theft of your intellectual property? If yes: do you know how it was obtained, and by whom? What steps did you take to prevent future compromise?

21. To your knowledge have any of your suppliers or partners been compromised or been victims of a security breach? If so: do you know why they may have been targeted, and by whom?

22. Do you know all your suppliers and others (e.g. brokers, shippers, logistics firms) in the import/export of your research or product?

23. Have you attended any conferences related to your research and if so, have you had any interactions with other attendees that raised your suspicions? Did any new contacts reach out before or after?

Additional guidance on how to assess and mitigate the risks to your research, development, and intellectual property is available from the Government of Canada. Please see the Safeguarding Your Research Portal.