Government of Canada | Gouvernement du Canada

Canada

Annual Report on the Implementation of Research Security Policies within the Federal Granting Agencies and the Canada Foundation for Innovation

2023-2024

This publication is available online at https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/additional-resources/annual-reports/annual-report-2023-2024.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/publication-request or contact:

ISED Citizen Services Centre

Innovation, Science and Economic Development Canada

C.D. Howe Building

235 Queen Street

Ottawa, ON K1A 0H5

Canada

Telephone (toll-free in Canada): 1-800-328-6189

Telephone (international): 613-954-5031

TTY (for hearing impaired): 1-866-694-8389

Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Email: ISED@canada.ca

Reproduction Authorization

Cat. No. Iu35-2E-PDF

ISSN 2819-0076

Aussi offert en français sous le titre Rapport annuel sur la mise en œuvre des politiques en matière de sécurité de la recherche au sein des organismes subventionnaires fédéraux et de la Fondation canadienne pour l'innovation.

Table of Contents

Message from the Minister of Industry, the Minister of Public Safety, and the Minister of Health

The Government of Canada recognizes the critical role that research plays in the advancement of knowledge, innovation, and societal development. Collaborations among domestic and international researchers are important to ensuring that Canadian world-class science and research remains on the cutting-edge of research and innovation.

To preserve this collaborative and open approach to science and discovery, the federal government remains committed to protecting Canada's research and intellectual property from theft, espionage, and foreign interference. Doing so is critical to the growing our world-class research and science ecosystem and intellectual property-intensive businesses. Security and openness are not mutually exclusive. Rather, they both contribute towards ensuring trust, integrity, and reciprocity in a collaborative and open research ecosystem.

The operationalization of Canada's federal research security policies is founded on transparency, procedural fairness, collaboration, and academic freedom. In applying the National Security Guidelines for Research Partnerships (the Guidelines) and the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy), the federal government aims to build trust and avenues for information sharing between post-secondary institutions and the federal government. This seeks to ensure that researchers feel comfortable approaching the government to inquire or disclose potential risks associated with their research projects, partnerships, or affiliations, and seeking advice on mitigating those risks.

The Government continues to roll out the Guidelines in research partnership programs across the granting agencies, as well as the STRAC Policy, to integrate research security into the development, evaluation and funding of federal grant applications. Ultimately, our objective is to inform the research community of the potential risks, while helping them adjust their day-to-day practices in a way that safeguards Canadian research. The effective integration of research security due diligence is an evolving process, and the Government of Canada is committed to protecting and maximizing the benefits to Canada and Canadians of our ongoing investments in science and research.

The Honourable Mélanie Joly, Minister of Industry

The Honourable Gary Anandasangaree, Minister of Public Safety

The Honourable Marjorie Michel, Minister of Health

1. Introduction

Purpose and scope of the Annual Report

The second *Annual Report on the Implementation of Research Security Policies within the Federal Granting Agencies and the Canada Foundation for Innovation* (the Annual Report) includes information on the results, key findings, and lessons learned that are associated with this year's implementation of the *National Security Guidelines for Research Partnerships* (the *Guidelines*). The report also highlights other initiatives and policies that are underway to safeguard Canadian science, data, and research, including the *Policy on Sensitive Technology Research and Affiliations of Concern* (STRAC Policy).

This year's Annual Report focuses primarily on the *Guidelines*, given that the STRAC Policy was recently enacted in May 2024 and results on its impact will not be available until an entire fiscal year has elapsed. For that reason, the 2024-2025 Annual Report will include results on the STRAC Policy's first year of implementation.

Importance of monitoring emerging risks to Canadian science and research

Due to the advanced nature of Canada's science and research sector, it can be an attractive target for those seeking to steal, use, and adapt our country's research for their own priorities and gains. In some cases, sensitive research can be exploited and used to advance the military, national defence, or state security capabilities of other countries, or to purposefully elicit harm. For those reasons, it is important to monitor these types of risks to prevent unintended consequences such as the loss of research data, diminished trust in research data and results, tarnished reputation, loss of potential future partnerships, and legal ramifications. While openness and collaboration are the cornerstones of scientific discovery, vigilance can prevent costly losses.

Proactive monitoring helps to ensure that Canada's science and research enterprise remains resilient, adaptable, and innovative in an ever-changing and competitive global landscape. The identification of emerging risks and implementation of appropriate mitigation measures is a shared responsibility between all levels of government, researchers, academic institutions, and funders. The federal government continues to work with partners across the science and research community to raise awareness on research security, and the importance of engaging in reliable and trusted research partnerships and collaborations. Ongoing collaboration between researchers and the Government of Canada is crucial for the large-scale and successful implementation of research security measures, including the *Guidelines* and the STRAC Policy.

Effective risk monitoring also allows for the identification and mitigation of risks that may jeopardize the openness and integrity of our country's research ecosystem. The objective is to ensure that Canadian research remains transparent and inclusive, as the federal government is committed to fostering a research enterprise where all Canadians can contribute to scientific advancements. Upholding common values and principles on research security and research integrity enables Canadian researchers to develop and maintain mutually beneficial collaborations with national and international research partners. These collaborations ultimately provide Canadians with the ability to benefit from the economic, environmental, and societal benefits of world-class research.

Overview of Canada's approach to research security

The Government of Canada is committed to building a robust research security culture by promoting due diligence efforts, risk mitigation practices, and open dialogue. This approach allows for the development of tailored, coordinated, and complementary research security measures that span across the government and the research community.

Canada's approach to research security focuses on practices that are risk-targeted and appropriately scaled. Risks can materialize in different ways and to varying degrees, and one-size-fits all safeguards can have adverse impacts on scientific research. Tailored research security practices allow stakeholders to work together to proactively identify, assess, and mitigate risks in order to protect the inputs, processes, and products that are part of scientific research and discovery without stifling innovation. In doing so, research security practices can enhance risk awareness among researchers, while respecting the foundations of academic freedom, scientific openness, transparency, trust, and reciprocity.

The Government of Canada's approach to research security follows the principles of Equity, Diversity, and Inclusion (EDI), and is based on the notion that freedom from discrimination and anti-racism are fundamental for a prosperous research enterprise. The diversity of Canada's research ecosystem is it's greatest strength, as it allows for new perspectives, increased creativity and innovation, and improves our ability to address complex problems. By adopting a country-agnostic approach, paired with case-by-case risk assessments, the government is able to account for threats that originate from anywhere in the world, while also actively taking steps to prevent Canada's research security measures from leading to discrimination or racial profiling within the research community.

2. Canadian Advancements in Research Security

The Government of Canada continues to take concrete measures to protect cutting-edge Canadian research, development, data, and technology, which are being actively targeted by foreign state actors to advance their security interests.

Current policies for safeguarding science and research

National Security Guidelines for Research Partnerships

The *National Security Guidelines for Research Partnerships* (the *Guidelines*) were developed and published in July 2021 by the Government of Canada, in consultation with members of the academic community, to incorporate national security considerations into the development, evaluation, and funding of research partnerships. While the *Guidelines* can be used by any researcher considering a research partnership, their application is a requirement for select federal funding programs for research projects with a private sector partner.

A key component of the *Guidelines* includes the Risk Assessment Form, which researchers can use to identify and assess risks that their research partnerships may pose to Canada's national security. The Risk Assessment Form asks two sets of questions that prompt researchers to consider the nature of their research (Know Your Research) and their proposed research partner organizations (Know Your Partner).

Implementation of the *Guidelines* began with a pilot phase, during which they were applied to the Natural Sciences and Engineering Research Council's (NSERC) Alliance Grants program. Innovation, Science and Economic Development Canada (ISED) and NSERC selected this program for the pilot phase due to its flexibility and because it receives funding applications in sensitive research areas that may carry higher national security risks (as defined in Annex A of the *Guidelines*). Following the conclusion of the *Guidelines'* pilot phase in July 2022, the Government of Canada began to gradually expand the application of this policy to additional federally funded research grant funding opportunities that support partnerships with the private sector.

To date, the *Guidelines* have been adopted by, and continue to apply to, the following federally funded private sector partnership programs:

- NSERC's **Alliance Grant**s program, including special calls and joint funding opportunities (pilot phase and ongoing);
- The Social Sciences and Humanities Research Council (SSHRC) and Canada Foundation for Innovation's (CFI) **Canada Biomedical Research Fund** and the associated **Biosciences Research Infrastructure Fund** (one-time call, implemented in March 2023 and funding was dispersed in March 2024);
- CFI's **2023 Innovation Fund** (as of October 2023);
- CFI's **Northern Fund** (as of January 2024);
- NSERC's **Idea to Innovation – Phase II** projects (as of June 2024);
- CFI's **John R. Evans Leaders Fund – Unaffiliated Stream** (as of June 2024); and
- The Canadian Institutes of Health Research's **Project Grants** (as of June 2024).

The ongoing expansion of the *Guidelines* adopts a risk-based approach that sequentially targets fields of research of highest risk within the federal granting agencies and the CFI. It will continue to focus on projects involving private sector partners.

Policy on Sensitive Technology Research and Affiliations of Concern

To build on the effectiveness of the *Guidelines*, the Minister of Industry alongside the Minister of Public Safety and Minister of Health, announced in January 2024 the *Policy on Sensitive Technology Research and Affiliations of Concern* (STRAC Policy). This policy specifies that "[g]rant applications submitted by a university or affiliated research institution to the federal granting agencies and the CFI involving research that aims to advance a sensitive technology research area will not be funded if any of the researchers involved in activities supported by the grant are affiliated with, or in receipt of funding or in-kind support, from a university, research institute or laboratory connected to military, national defense or state security entities that could pose a risk to Canada's national security."

To support the implementation of this new requirement by the research community, the Government of Canada published two lists. The first is a list of Sensitive Technology Research Areas (STRA) that outlines emerging technologies and research areas that have novel applications or capabilities, where transfer out of Canada or use by foreign entities could cause injury to Canada's national security or defense. The second list is the List of Named Research Organizations (NRO), composed of research organizations and institutions that pose the highest risk to Canada's national security due to their direct, or indirect connections with military, national defence, and state security entities. The STRA and NRO lists operate in conjunction, which means that affiliations with and funding or-kind support from NROs are only of concern in the context of research that aims to advance a sensitive technology research area; Public Safety Canada (PS) developed these two lists and will update them at regular intervals.

The STRAC Policy and its requirements apply in a harmonized manner to applicable funding opportunities of the federal granting agencies and the CFI, launching on or after May 1, 2024. More detailed information to support this implementation, including forms and procedures, were published in March 2024 by the federal granting agencies and the CFI.

Researchers must nonetheless remember that the NRO List contains the highest risk institutions, and other institutions not included on the NRO list may still pose a risk to Canada's research. As such, researchers should apply due diligence practices to mitigate risks that may be associated with collaborations or partnerships in sensitive technology research areas, even when STRAC does not apply.

New and existing tools that support researchers in safeguarding Canada's research ecosystem

The Government of Canada is actively developing new resources that aim to protect our country's science and research enterprise.

ISED launched the Safeguarding Your Research Portal in 2020, after extensive consultations with federal departments and agencies and the research community. The platform is updated regularly with new guidance and resources to provide information to the Canadian research community on how to safeguard its research and assets, including training courses, briefing videos, checklists, guides, and case studies.

ISED added several new resources to the Safeguarding Your Research Portal in the 2023-2024 fiscal year, including:

- An online training course on "Safeguarding Research Partnerships with Open Source Due Diligence";
- Emerging Technology Trends Cards, developed by Defence Research and Development Canada (DRDC), which communicate information about technologies that may impact defense, public safety, and national security;
- A guide on "Safeguarding Research in Canada: A Guide for University Policies and Practices" that was developed by the U15 Group of Canada's most research intensive universities;
- The "G7 Best Practices for Security and Open Research", which offers examples of research security and integrity best practices; and
- Guidance on "Integrating Security Considerations into Procurement of Research Goods and Services", which aids in identifying risk within a procurement and helps individuals responsible for procurement related to research projects mitigate risk.

Furthermore, the Safeguarding Your Research Portal continues to align its available guidance with other avenues of support that are offered to the research community. To ensure that researchers and academic institutions are aware of Canada's federal research security policies and requirements, the granting agencies co-developed a Tri-agency Guidance on Research Security webpage, which is housed on NSERC's website. Similarly, the CFI published a Research Security webpage that explains how Canada's federal policies apply to their funding opportunities. Overall, both these websites provide more detailed guidance on how to comply with the *Guidelines* and STRAC Policy.

Outreach efforts and continuous engagement with Canada's research community

Canada's Research Security Centre (the Centre) is housed at PS and has been operational since summer 2023. The Centre employs regional advisors across Canada, who provide direct support to the Canadian research community on matters relating to research security. The Centre provides assistance on research security risk identification and risk mitigation, with the intent of building a robust research security culture among the academic community. In addition, the Centre supports collaboration on research security between the federal government and the provinces and territories. In 2023-2024, PS observed that there was a strong desire for Safeguarding Science (SASC) workshops across the post-secondary community, for enhanced coordination between federal and provincial policies, and for the development of appropriate tools tailored to universities' realties in order to raise awareness on research security. PS continues to lead the Safeguarding Science initiative, which provides interactive workshops for Canadian universities and the broader research community to equip them with the knowledge and tools required to protect their valuable research. As of February 2024, PS, through the Research Security Centre, has leveraged expertise from across Government of Canada to deliver 10 Safeguarding Science workshops, reaching 59 academic institutions, 16 research institutions, 5 other federal departments, totaling to more than 1043 total participants.

The Canadian Security Intelligence Service (CSIS) routinely engages with academia, research institutions, and private sector organizations that participate in research and innovation to increase awareness of, and resilience to, threats to research security. This engagement includes bilateral discussions, threat briefings, and sharing guidance documents and other information. CSIS aims to increase awareness of state-sponsored espionage threats targeting these sectors and lay the groundwork for reciprocal partnerships that will help protect Canadian research and development, and ensure Canadians and the Government of Canada have secure access to leading-edge and trusted technology. CSIS worked closely with academic institutions across Canada to share information about national security threats to help safeguard Canadian research and information from economic espionage activities. In 2023, CSIS conducted in-person campus visits to over 13 Canadian academic institutions to engage with senior leadership and administration, faculty, and staff.

The Communications Security Establishment Canada (CSE) houses the Canadian Centre for Cyber Security, which regularly holds sector community calls, to share threat information, trends and maintain an ongoing dialogue on cyber security. CSE also publishes advice and guidance on a range of topics such as cyber hygiene, spotting malicious emails, recognizing and avoiding phishing attacks, and protecting against malware. To further cyber security awareness among the research community, CSE also offers a range of courses via the Learning Hub aimed at academia, including: Introduction to Research Security, Cyber Security for Researchers, and Cyber Security Risks for Travelling University Employees.

NSERC houses the Tri-agency guidance on research security and continues to engage with the research community to ensure researchers clearly understand the requirements that apply to their grants, while supporting capacity building and research security best practices across post-secondary institutions by delivering outreach sessions with individual institutions and hosting dedicated office hours for Research Grant Officers. Canada's federal granting agencies and departments also continue to actively participate, host, or lead engagements in major conferences or panel discussions on the topic of research security. This includes participation in events organized by the Canadian research security community, such as the 2023 Research Security Conference co-hosted by the University of Calgary and University of Alberta, as well as international conferences such as the 8th Academic Security and Counter Exploitation organized by Texas A&M University (USA) where NSERC, PS, and Global Affairs Canada (GAC) participated alongside representatives from dozens of Canadian post-secondary institutions.

More specifically, these government officials participated in multiple panels on Canada's approach to research security and held bilateral meetings on the margins with officials from other participating countries.

The Government of Canada-Universities Working Group is the primary policy interface between the Government and Canada and the university community. The working group was established in 2018 to collaboratively identify, share, and promote best practices to mitigate security risks and to protect data and intellectual property. In the past fiscal year, this working group met regularly and continues to co-develop resources for implementation in the university sector, in response to emerging issues across the Canadian research ecosystem.

Building on the work of the Government of Canada–Universities Working Group, a complementary group was established in 2023 to discuss challenges and risks that are unique to colleges, polytechnics and CÉGEPs. The Colleges, Polytechnics, and CÉGEPs Working Group facilitates information-sharing between institutions, federal funding agencies, the CFI, and government departments to identify research security measures that are tailored for this sector. Work remains underway to determine the timing and approach to integrate research security into this sector.

The Government of Canada also recognizes the important role that research organizations and funders play in strengthening Canada's research ecosystem. The Strategic Science Fund (SSF) continues to provide funding to Canadian not-for-profit science and research organizations, which bolsters the competitiveness of Canada's research by furthering the exchange of knowledge and it accelerates the recruitment of world-class talent. To ensure that SSF recipients safeguard their work, and the work they support, the Government of Canada has integrated research security requirements—consistent with the *Guidelines* and STRAC Policy—into the Contribution Agreements of these organizations. This funding precondition requires the development and submission of a Research Security Plan—a document that demonstrates how the organization will integrate national security considerations into their funding and research practices. To support these organizations in drafting and operationalizing their Research Security Plans, the Government of Canada published, and has recently updated, the "Guidance for Research Organizations and Funders on Developing a Research Security Plan". This guide continues to provide information on how research organizations and funders can identify, assess and mitigate national security risks in a systemic, consistent, and documented manner.

Aligning research security policies and practices at the federal, provincial, and territorial level

The federal government recognizes the important role that provincial and territorial governments play in supporting research in Canada. For that reason, ISED engages regularly with these jurisdictions to share information, in an effort to align and coordinate efforts where possible. Alignment where possible across Canada's different jurisdictions serves to minimize potential administrative burdens associated with implementing multiple research security requirements. Such consistency is equally an important consideration across federal departments and agencies that fund or conduct research, to collectively prevent malicious actors from exploiting gaps.

Collaborating with international partners on research security best practices

Internationally, Canada continues to work closely with allies and various organizations to further develop our evidence-informed and comprehensive strategy to research security. Notably, Canada's ongoing engagement through the Group of Seven (G7) and the Organisation for Economic Co-operation and Development (OECD) have served to advance and establish meaningful research security activities.

The government continued to promote the work of the G7's Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE), including the G7 Common Values and Principles on Research Security and Research Integrity published in June 2022 and the G7 Best Practices for Secure and Open Science published in February 2024. We also promoted Canadian participation in the G7's Virtual Academy, launched in spring 2023, which offers a library of documents, guidance, legislation, and resources to be shared amongst the international research community. Other international engagements include Canada's participation in the OECD's annual Global Science Forum (GSF). The objective of the GSF is to support member countries in improving their science policies, while providing a venue for consulting and sharing in the benefits of international research collaborations. In the context of this forum, the Government of Canada is committed to further exploring how research security considerations can be integrated into the following GSF long-term priorities:

- Research infrastructure policy;
- Research workforce of the future;
- Trust in science and citizen science; and
- Integrity and security in the global research ecosystem.

The Government of Canada also actively participates in the Five Country Ministerial, a forum for the Five Eyes security ministers to meet and discuss opportunities for collaboration across the full range of public safety and national security issues facing each of the Five Eyes partners. Throughout 2024, the Five Countries have collaborated and advanced efforts on a range of issues, including research security. The Five Countries recognise the need to mitigate the threat posed by foreign interference and espionage within our research ecosystems, and remain committed to exchanging best practices and threat information on research security, including how foreign entities of concern may be attempting to adapt to and bypass safeguards, to improve the resilience of those ecosystems.

In addition, NSERC regularly collaborates with international funding agencies — including through the Global Research Council, of which it is a founding member — to strengthen global alignment on policy priorities such as research integrity and security, in order to foster multilateral research and collaboration across continents.

Lastly, Global Affairs Canada (GAC) continues to lead the Government of Canada's participation in the Multi-Country Dialogue on Research Integrity, with participation from Australia, New Zealand, the United States, and the United Kingdom. This collaborative forum provides participating countries with an opportunity to share best practices in addressing foreign interference in research, with a view to strengthening the integrity of the global research ecosystem. In the past fiscal year, this group held an in-person dialogue with Canadian academia in Ottawa, whereby representatives from Canada's university community were invited to present and engage directly with national delegations from the participating countries. Key themes that were discussed included: mechanisms for government-academia coordination, international research collaboration, the importance of diversity, equity, and inclusion, and upcoming research security events. The Government of Canada also continues to raise research security issues in its bilateral engagements with foreign partners, including via its established system of Joint Science and Technology Cooperation Committees (JSTCCs). These exchanges of information are

important for building trust and co-operation between the federal government, academia, and Canada's allies.

3. Tracking the Impact of Canada's *National Security Guidelines for Research Partnerships* and supporting efforts

Measuring the impact of Canada's research security policies and practices

To measure the impact of Canada's federal research security policies and practices, the government developed a Performance Measurement Strategy (PMS). It provides ISED, the federal granting agencies, the CFI, and national security departments and agencies with a framework for assessing the performance of Canada's research security policies. The PMS uses a set of performance indicators to assess progress towards a series of short-, medium-, and long-term outcomes, which collectively measure how the *Guidelines* and their supporting efforts contribute to advancing the federal government's commitment to protecting Canada's national security and research enterprise.

The main data sources for this reporting process are the internal databases of the federal granting agencies, the CFI, and national security departments and agencies, as well as the results from ISED's annual and voluntary Research Security Survey.

Outlining the scope of this year's reporting cycle

The inaugural Progress Report on the Implementation of Canada's *National Security Guidelines for Research Partnerships and Supporting Research Security Efforts* was published in January 2024, and included results on the *Guidelines*' pilot phase which took place from July 2021 to July 2022. The 2023-2024 Annual Report covers data that was collected from July 2021 to March 31, 2023, (referred to hereinafter as Year 1), and from April 1, 2023, to March 31, 2024 (Year 2).

Following this inaugural report, the Government of Canada intends to publish the results for each fiscal year via an annual report. The results included in this year's Annual Report therefore represent data collected from April 1, 2023, to March 31, 2024 (referred to hereinafter as Year 2), and is representative of the federal funding opportunities that implemented the *Guidelines* during this time[1].

Specifically, the results captured in this year's Report represent NSERC's Alliance Grants program, including special calls and joint funding opportunities,as well as SSHRC and CFI's Canada Biomedical Research Fund and the Biosciences Research Infrastructure Fund (CBRF-BRIF). This year's reporting cycle excludes the results from CIHR's Project Grant competition, given that the data is not yet available, as the competition is ongoing. The report also does not

[1] For more information on the specific funding opportunities that have applied the *Guidelines* as of March 31, 2024, please reference the section above titled "Current policies for safeguarding science and research".

include CFI's 2023 Innovation Fund and the CFI's Northern Fund, because the data on these programs is not sufficiently complete to be reported on at this time. CFI's framework for implementing the *Guidelines* had not yet been finalized when the Innovation Fund 2023 was launched in October 2021. As a result, ISED, CFI, and Canada's national security partners decided that the policy would be applied retroactively. The application deadline for Innovation Fund 2023 was in July 2022, and the *Guidelines* were applied in October 2023 for risk assessments to be completed prior to contract award. As of March 31, 2024, CFI had not received all the requested Risk Assessment Forms. Regarding CFI's new Northern Fund, the program was launched in January 2024 and the *Guidelines* were applied at that time. As of March 31, 2024, CFI had not yet received any applications for their Northern Fund. Therefore, the results of research security assessments in these programs will be included in the 2024-2025 Annual Report. Given that the new STRAC Policy only came into effect in May 2024, its results will be covered in the 2024-2025 Annual Report to be published in late fall 2025.

Summarizing the results of the *National Security Guidelines for Research Partnerships* for Year 2

Between April 1, 2023, and March 31, 2024, a total of 1140 research partnership applications were subject to the *Guidelines*. Of these applications, 691 were funded where any risks identified were deemed to be mitigable by the risk mitigation plans developed by the applicants and their institutions. In addition, 9 applications were issued funding contingent on the implementation of additional mitigation measures. Only 4 applications were not awarded funding due to unmitigable national security risks, while 72 were returned for administrative reasons, and 364 were not awarded after merit review.

Figure 1. Funding outcomes for all applications subject to the *National Security Guidelines for Research Partnerships* in Year 2

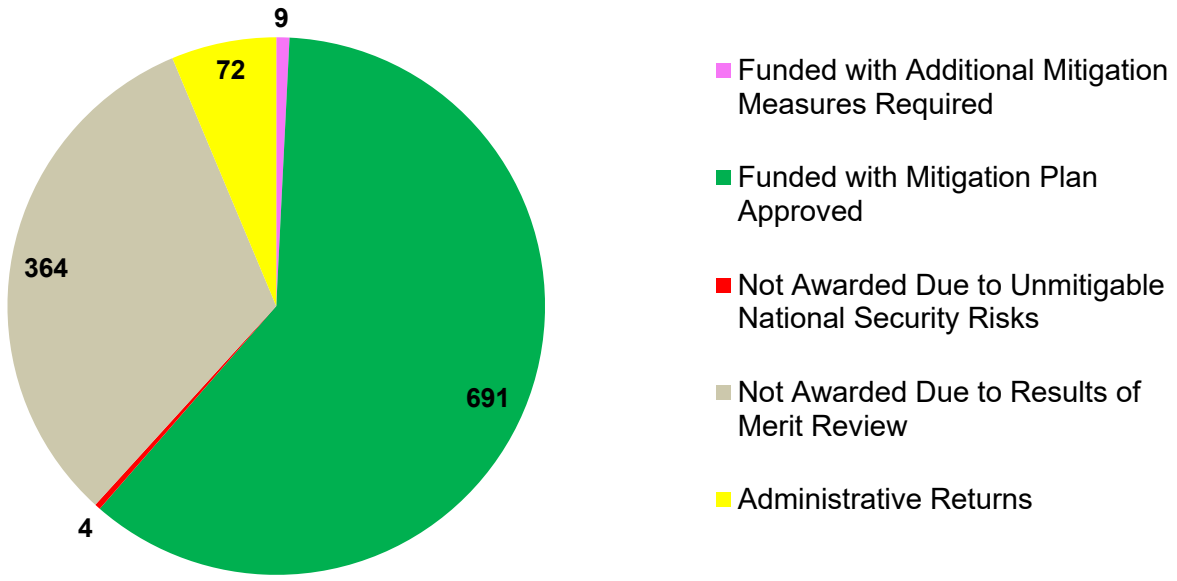

Figure 1. Funding outcomes for all applications that were subject to the National Security Guidelines for Research Partnerships. *The chart provides a collated and visual representation of the funding results for NSERC Alliance Grant applications, as well as SSHRC and CFI's*

CBRF-BRIF applications, that were subject to the Guidelines between April 1, 2023, and March 31, 2024.

It is important to note that approximately 65% of all applicants had accurately identified the risks to their proposed research project. This represents a significant improvement from last year, where only 47% of applicants had accurately identified their risks within the Risk Assessment Form. This suggests that Canada's research community has a growing ability to accurately identify the risks specific to their research, while also correctly implementing the *Guidelines* themselves. Moreover, 82% of all successful applicants identified, and included, appropriate risk mitigation measures in their Risk Assessment Form. This demonstrates that, in many cases, the risk mitigation plans proposed by applicants were sufficiently robust to address risks associated with their projects even if they had not identified all potential risks at the outset.

In addition to that, these findings are comparable to the results from Year 1:

Figure 2. Funding outcomes for applications subject to the *National Security Guidelines for Research Partnerships* in Year 1 & Year 2

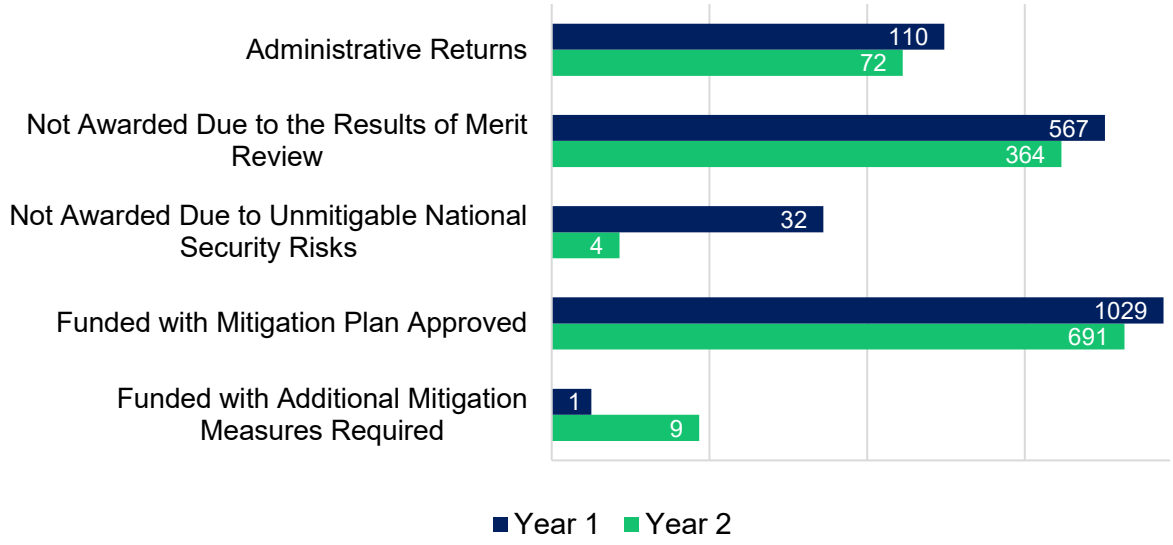

Figure 2. Funding outcomes for all applications subject to the National Security Guidelines for Research Partnerships in Year 1 & Year 2. *The chart provides a visual comparison of the funding results for the applications that were subject to the Guidelines in Year 1 (July 2021 – March 31, 2023) versus Year 2 (April 1, 2023 - March 31, 2024).*

Funding outcomes for applications that were referred for a national security review in Year 2

Of the 1140 applications that were subject to the *Guidelines*, the granting agencies and CFI referred 24 (approximately 2% of applications) to PS for a national security review. Fourteen (14) were referred from the NSERC Alliance Grants program, whereas 10 originated from CBRF-BRIF. In 4 cases, PS found that the research partnership could pose an unmitigable risk to Canada's national security and/or research ecosystem. Accordingly, the granting agencies did not

fund these projects. In 7 cases, PS found that the research partnership posed a low risk to Canada's national security, accounting for the mitigation plan provided by the applicant. Accordingly, the granting agencies funded these projects.

Finally, in 13 cases, the research partnership was deemed to present risks that were not sufficiently addressed by the risk mitigation plan provided but could be mitigated with additional risk mitigations measures. Only 9 of these 13 applications were funded; this is because for CBRF-BRIF, the national security review was conducted prior to the merit review process and, subsequently, SSHRC withdrew 4 of the applications that it had referred once it was determined that these applications did not pass the granting agency's merit review stage.

Please refer to Figure 3 below for a description of funding results and outcomes for all applications that required a national security assessment, and Figure 4 for a breakdown of this same data by funding program (NSERC Alliance Grants and CBRF-BRIF).

Figure 3. Funding outcomes for applications that ***did*** require a national security assessment in Year 2

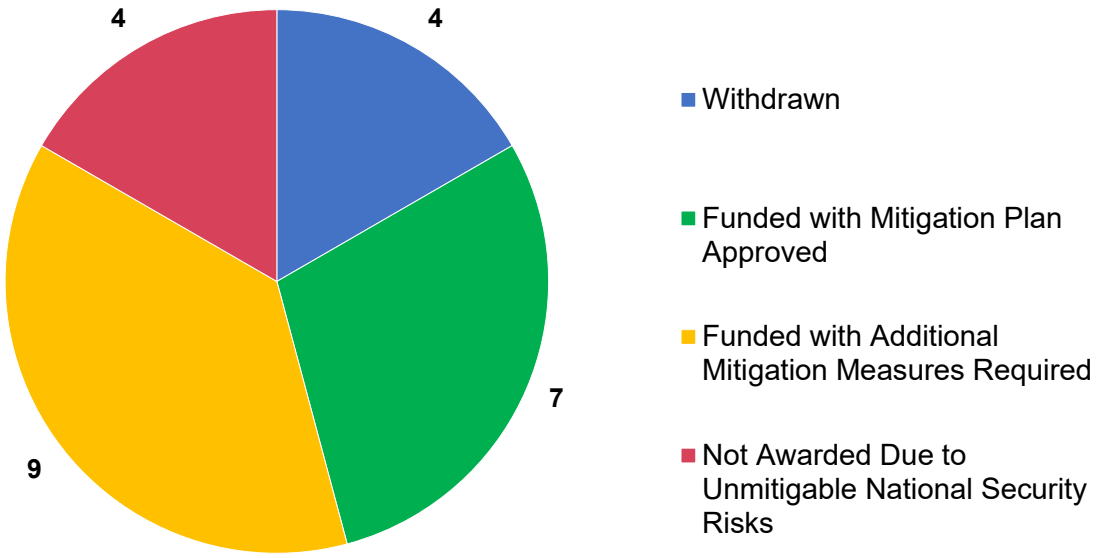

Figure 3. Funding outcomes for all applications that did require a national security assessment. The chart provides a collated and visual representation of the funding results for NSERC Alliance Grant applications, as well as SSHRC and CFI's CBRF-BRIF applications, that did require a national security assessment between April 1, 2023, and March 31, 2024

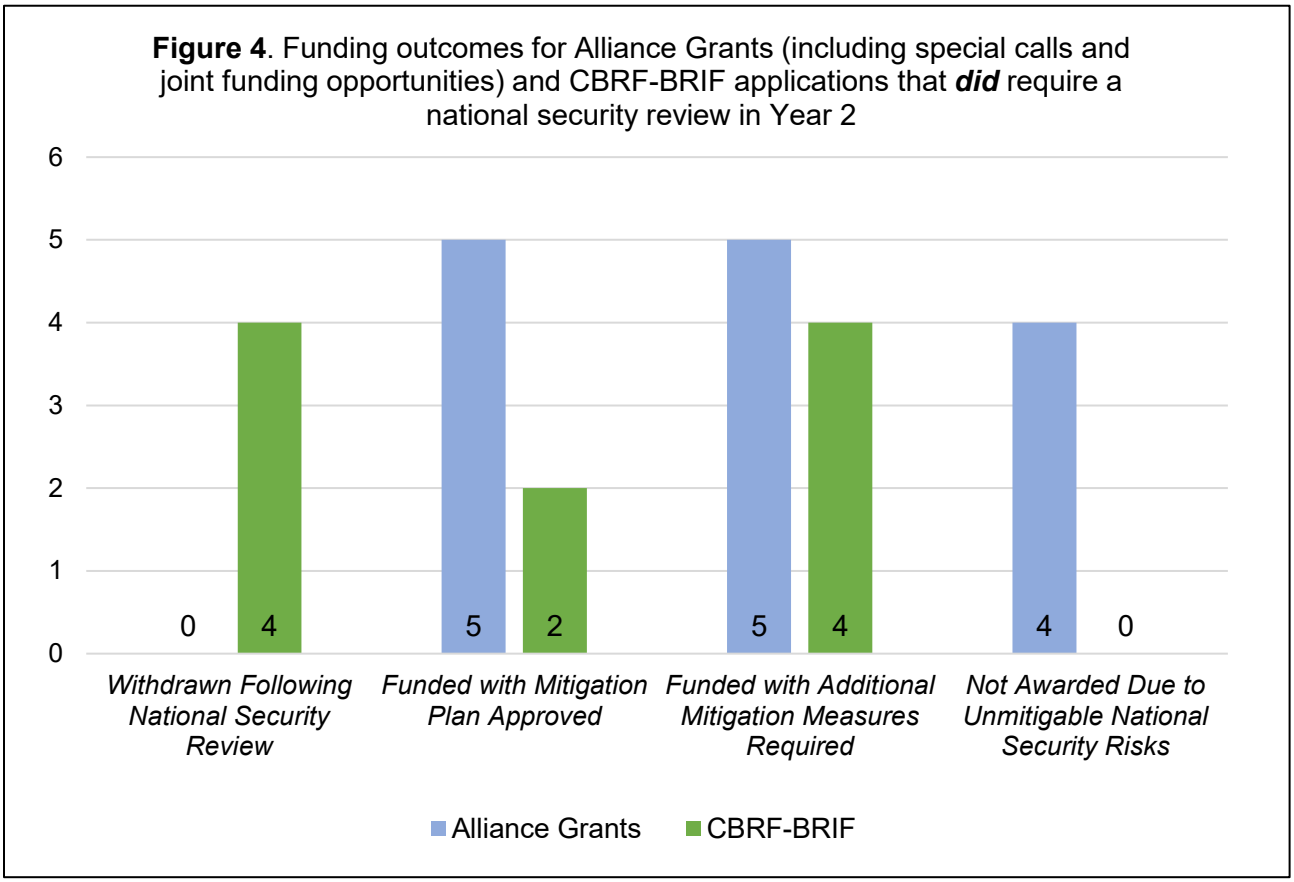

Figure 4. Funding outcomes for Alliance Grant and CBRF-BRIF applications that did require a national security assessment. The chart provides a visual representation of the funding results NSERC Alliance Grant applications as well as SSHRC and CFI's CBRF-BRIF applications that required a national security assessment between April 1, 2023, and March 31, 2024. The findings displayed in this visual are organized based on four possible outcomes: funded without, funded with conditions, not awarded due to national security risks, and application withdrawn after national security review was conducted.

NSERC, PS, and national security partners noted a set of common risk factors that were present among the applications not funded as a result of the national security assessment process. These were research partnerships where the nature of the research was considered to be sensitive and where the private sector partner organization has public ties to foreign states known to target academic institutions, the private sector, and the general public.

Impact of the *National Security Guidelines for Research Partnerships* on the diversity of applicants and partner organizations

A) Alliance Grants (including special calls and joint funding opportunities)

The *Guidelines* had a negligible impact on the diversity of partner types that were involved in projects receiving funding through Alliance. This is reflected by consistency in the percentage of

partners from the private, public, and not-for-profit sectors that were submitted in applications between Year 1 and Year 2:

Participation by partner sector	Private	Public	Not for Profit
Year 1 (July 2021 - March 2023)	65%	19%	13%
Year 2 (April 2023 - March 2024)	66%	21%	13%

The Government of Canada also continues to monitor Canada's federal research security policies to ensure that they do not unintentionally contribute to prejudice or discrimination against researchers who identify as a visible minority, or in the way research funding is distributed.

To date, the *Guidelines* have had no discernable impact on the diversity of applicants who received funding through Alliance from Year 1 to Year 2. This is reflected in the application success rates, which have increased since last year for applicants who self-identified as a visible minority[2]:

Success rate of self-identified visible minorities	***Year 1*** (July 2021 - March 2023)	***Year 2*** (April 2023 - March 2024)
	59%	70%

B) CBRF-BRIF

CBRF-BRIF's success rate for self-identified visible minorities was approximately 19%. For additional information on SSHRC's 2023 success rates for visible minorities for comparison, please refer to their public dashboard which reports on EDI data for their core funding opportunities

It is important to the note that CBRF-BRIF was a new and *one-time* funding opportunity that was administered by SSHRC and CFI between May 2022 and March 2024. This was the only application cycle, and as a result, there is no available EDI data, or data on the diversity of partners, from previous years that can be used as a comparison.

In terms of the diversity of partners submitted within CBRF-BRIF applications, it can be summarized as follows:

[2] Data on the success rates for self-identified visible minorities has been organized by program, given that each funding opportunity has a different baseline of comparison (i.e., the grant's success rate for self-identified visible minorities prior to the implementation of the *Guidelines*).

Participation by partner sector	Private	Public	Not for Profit
Year 2 (April 2023 - March 2024)	67%	14%	19%

Impact of the *National Security Guidelines for Research Partnerships* on the service standards for the assessment of applications

The federal government continues to refine and adjust the process for evaluating applications that are subject to the *Guidelines*. The goal is to minimize the *Guidelines'* impact on the CFI's and the granting agencies' service standards for issuing funding decisions. To identify where possible delays are taking place, and what changes might be needed to improve service standards, this report has divided the results on service standards into two categories: applications that did require a national security assessment from PS, versus the applications that did not.

For Year 2, approximately 74% of NSERC's funding decisions for Alliance Grants that were subject to the Guidelines but did not require a national security assessment were made within its standards, whereas approximately 14% of funding decisions that did require a national security assessment were issued within its service standard. This reflects the fact that national security assessments typically occur after the merit review process, while NSERC's service standards have been based on the merit review process. Within the next year, NSERC will be adjusting its service standards to more clearly incorporate the 10 weeks that are required for the national security review of applications referred to Public Safety Canada following the completion of the merit review process; this will enable more accurate reporting against more realistic service standards, that take into account this critical element of the decision-making process. All of CBRF-BRIF's decisions (100%) were made within SSHRC's and CFI's service standards, as any applications requiring a national security review were referred to Public Safety Canada prior to the completion of the merit review process.

4. Research Community Feedback and Efforts

In recent years, the Government of Canada has been working with Canada's academic research community to raise awareness of the importance of research security. Through these ongoing engagements, the government has observed a growing appreciation towards Canada's approach to safeguarding research, data, and technology.

Key findings from the 2024 Research Security Survey

This year's Research Security Survey had a total of 155 respondents, and the results indicate that awareness of security risks amongst Canada's research community has increased since the implementation of the *Guidelines*. More specifically, the survey results show that 84% of respondents feel 'prepared' or 'very prepared' to implement the *Guidelines*, including the completion of its Risk Assessment Form, in comparison to 75% in Year 1. In addition, 75% of survey participants agreed that their awareness of the risks associated with research partnerships had increased in Year 2, versus 62% in Year 1. To ensure this progress year-over-year, the

Government of Canada will continue to work with the research community to raise awareness on the importance of research security, while providing guidance on how to implement the *Guidelines.*

The survey also provided useful feedback on the federal government's Safeguarding Your Research Portal, and its available tools and training courses. For instance, respondents offered a series of suggestions, including adding case studies and current examples to the portal and improving the usability and accessibility of the platform's resources and training courses.

The Government of Canada intends to proceed with a number of planned updates towards the Safeguarding Your Research Portal. This will include the publication of new case studies that focus on procurement of equipment and foreign talent recruitment programs. Furthermore, ISED is in the process of enhancing the design of the portal, in an effort to improve the website's navigation and organization of resources. The federal government continues to update, add, and revise the tools and information that are offered on the portal, to ensure that the research community has current and relevant guidance.

In addition to ISED's 2024 Research Security Survey, PS conducts surveys following the delivery of Safeguarding Science workshops. Participants of these workshops are encouraged to provide feedback and comments on the particular module they attended. These modules provide information on topics like Research Security, Dual Use, Exports Controls and Immigration processes. The results often display a 75% rate of meeting the training expectations of the participants including a rate of 89% of participants indicating that these workshops have raised their awareness of the importance of research security. Where the feedback indicated areas upon which to improve, PS endeavored to incorporate these comments into future versions of the Safeguarding Science workshops.

Additional feedback from the research community

Following consultations with the research community, the Risk Assessment Form was updated in March 2023 to a streamlined format, including specific guidance to assist with responding to each question. Researchers and administrators have shared positive comments regarding the form's improved usability and its harmonized implementation for all relevant federal funding opportunities.

Researchers and administrators are requesting more guidance on developing robust mitigation plans. While the feedback indicates that several institutions have put in place institutional-level processes and tools to help their researchers integrate risk mitigation measures, this could be bolstered through additional guidance tailored to identifying appropriate project-specific mitigation measures.

Many researchers and administrators have also expressed confusion regarding the appropriate contact points to ask questions about research security, the Government of Canada's policies, and the requirements that apply to applications submitted to the granting agencies or the CFI. Questions should be directed to the appropriate funding organization if they relate to the research security requirements that apply as part of a grant application or to an awarded grant from that organization; appropriate contact information can be found in the Tri-agency guidance on research security and in the guidance published by the CFI. Inquiries about the following topics should be directed to the Research Security Centre:

- Guidance on research security, including on how to safeguard research and associated best practices, as well as advice on any case-specific scenarios or concerns.

- The STRAC Policy, including the lists of Sensitive Technology Research Areas and Named Research Organizations.
- Guidance on how to terminate an affiliation with, or funding or in-kind support, from a Named Research Organization.
    - Guidance on how to apply due diligence practices and/or how to mitigate risks that may be associated with a collaboration or partnership that aims to advance a Sensitive Technology Research Area—whether or not the organization is listed in the most recent list of Named Research Organizations.

Academic institutions and the implementation of research security best practices

Budget 2022 provided an additional $125 million over five years, starting in 2022-23, with $25 million ongoing, to add research security as one of five priority areas supported under the Incremental Project Grants (IPG) stream of the Research Support Fund (RSF). This investment continues to support eligible post-secondary institutions with identifying, assessing and mitigating potential risks to research security.

The financial support provided via the Research Support Fund continues to assist Canada's most research-intensive universities in a variety of ways, such as implementing cybersecurity improvements and hiring staff or experts for research security purposes. Through ISED's engagements with academic institutions, RSF recipients have indicated that institutions are prioritizing the use of research security funds for completing grant and award applications and research proposals, and for developing mitigation measures across risk areas.

During the 2022-2023 cycle, 48 (of the 49 eligible) academic institutions submitted applications for and received research security funding, totaling to approximately $24.72 million. This funding allowed eligible post-secondary institutions to:

- Hire new staff and support existing positions within the research enterprise that are focused on the research security threats including physical, cyber, partnerships, intellectual property, people;
- Assist principal investigators in developing granting and funding applications that comply with the *Guidelines*;
- Help researchers understand the criteria for national security related to sensitive technologies, and the levels of due diligence required to understand corporate partnerships and their associated networks;
- Assess research partnerships, protection of intellectual property, and the prevention of reputational damage; and
- Refine processes for research security, including the development of research forms, automated processes, and training sessions to educate faculty on the need for research security.

In addition, for this first cycle of RSF funding:

- A total of 143 projects were submitted in the 2022-23 application cycle.
- Institutions leveraged a total of approximately $11.24M in additional sources of funding (e.g., from institutional research funds) for 66 projects to support research security projects.
- Institutions indicated that 42 full-time equivalent (FTE) positions were established or supported (full-time and/or part-time) using research security funding

- Approximately 3,702 personnel received training and/or targeted information about research security including cyber security, on-campus protocols and new government advisories such as the *Guidelines*.

Institutions that are currently ineligible for research security funding through the IPG stream of the RSF are encouraged to explore mechanisms that allow for aggregating resources across multiple institutions to help address their research security needs. The Government of Canada encourages RSF recipients to use their research security funding to incubate research security capacity and resiliency across academic institutions of all sizes. Due in part to the financial support provided by the RSF, the federal government has also observed that a number of RSF-eligible institutions have come together to establish a community-driven network that includes research security administrators across 64 academic institutions in Canada, with a goal of supporting universities—large and small—by sharing information and best practices regarding research security, and organizing events and symposia to collaborate and better understand how the science community can safeguard their research effectively.

5. Concluding Remarks and Future Initiatives

The Government of Canada is committed to supporting a collaborative and open approach to science and discovery. The principles of open science are an essential part of innovative and collaborative research, and are indispensable to pushing the boundaries of science. We must continue to foster this openness and collaboration, which are the cornerstone of discovery, while addressing the need to safeguard the country's research from theft, espionage and foreign interference. Ultimately, Canada's research ecosystem should remain as open as possible, and as secure as necessary.

To further bolster Canada's research security framework, the federal government recognizes that additional efforts are required to ensure that all members of the research ecosystem are able to implement targeted safeguards that are specific to the risks that emerge within their field of science. To that end, the government will continue to roll-out the implementation of the *Guidelines* to additional funding organization programs, with particular focus in 2024-25 on NSERC's Idea to Innovation grants program (Phase II projects) and CIHR's Project Grants program, with plans for application in additional CFI programs followed by selected programs at SSHRC.

In addition, the government will monitor the implementation of the new STRAC Policy, including through the validation of the accuracy of a randomized subset of attestations received with applications that are aiming to advance a sensitive technology research area. Grant recipients will be expected to comply with the Policy for the duration of the grant following the versions of the lists that were publicly available on the date that the grant application was submitted. Outcomes of the validation process will be described in next year's 2024-25 Annual Report.

The government will continue to review the lists of Sensitive Technology Research Areas and the Named Research Organizations, as required, and any updates to either of these lists will be communicated in advance of their coming into force under the STRAC Policy. This will give researchers and their institutions will have time to review the updated lists and take appropriate action to comply with the Policy prior to submitting new grant applications to which the updated lists will apply.

As the threat landscape evolves, the government will continue to develop additional guidance and tools to support our collective Canadian responsibility to promote and protect open and

transparent research projects that are protected from unwanted knowledge transfer, including guidance on conflicts of interest and on the procurement of research goods and services.

Ultimately, all of Canada's research security measures—including the *Guidelines* and the STRAC Policy—are designed and intended to better safeguard Canadian research, intellectual property, data, and knowledge development. These measures aim to preserve the internationally collaborative and open approach to research and discovery, while also protecting Canada's interests in national security by ensuring that the appropriate protections are in place to maximize the benefits for all Canadians.