Government of Canada
Gouvernement du Canada

Canada

Progress Report on the Implementation of Canada's *National Security Guidelines for Research Partnerships* and Supporting Research Security Efforts

2021-2023

This publication is available online at https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/additional-resources/annual-reports/progress-report-2021-2023.

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. Iu37-41/2023E-PDF

ISBN 978-0-660-48256-9

Aussi offert en français sous le titre Rapport sur l’état d’avancement de la mise en œuvre des Lignes directrices sur la sécurité nationale pour les partenariats de recherche et de l’appui aux efforts de sécurité de la recherche.

Table of Contents

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

World-class research is made possible by domestic and international collaborations between researchers and research institutions, and in partnership with organizations from the public, for-profit, and not-for-profit sectors. To ensure we preserve this collaborative and open approach to science and discovery, the Government of Canada remains committed to protecting Canadian research and intellectual property against foreign interference, espionage, and theft.

The National Security Guidelines for Research Partnerships (the *Guidelines*) were introduced in July 2021, and developed in collaboration with the Government of Canada, universities, and associations that represent academic institutions. The *Guidelines* integrate national security considerations into the development, evaluation and funding of research partnerships in a way that ensures openness and research security are complementary and mutually reinforcing. These measures ensure that Canada's research ecosystem can remain as open as possible and as secure as necessary.

The pilot phase of the *Guidelines* was applied to the Natural Sciences and Engineering Research Council of Canada's (NSERC) Alliance grants program, for any application involving one or more private sector partner organizations. Through this pilot phase, NSERC developed and implemented new processes to integrate the *Guidelines* into the evaluation and funding of these partnerships.

From July 2021 to July 2022, approximately 4% of Alliance and Alliance Missions special call applications that were subject to the *Guidelines* (totalling 48 out of 1158 applications) required an assessment and advice from Canada's national security departments and agencies. Of these 48 applications, 32 were found to pose unmitigable risks and were therefore denied funding. Ultimately, a total of 59% of Alliance and Alliance Missions applications that were peer-reviewed and subject to the *Guidelines* (678 out of 1158 applications), received funding from NSERC, which is consistent with the number of successful Alliance applications prior to the implementation of the *Guidelines*. Any applicant who identified risks with their project was required to implement a risk mitigation plan for the duration of their research to address these risks. As a result, the implementation of the *Guidelines* has successfully integrated national security considerations into the funding of research partnerships with private sector partners, while not unduly affecting the success rate of the Alliance program compared to previous years.

When the *Guidelines* were released, the government stated its intention to expand their application in the near term to other federal programs administered by federal granting agencies – NSERC, Canadian Institutes of Health Research (CIHR), and Social Sciences and Humanities Research Council (SSHRC) – and the Canada Foundation for Innovation (CFI). Expanding the application of the *Guidelines* will provide greater assurance that federal research funding is not contributing to research partnerships that conflict with Canada's national security. The expanded application of the *Guidelines* will promote a greater security awareness culture in the overall research ecosystem which will help safeguard Canada's investments in science and innovation.

The lessons learned from the NSERC Alliance pilot phase will be applied and adopted throughout the next steps in further implementing the *Guidelines*. This next phase will be implemented gradually and will target funding opportunities in streams where the research involved is at risk of national security threats.

The expanded roll-out began in early 2023 with the Canada Biomedical Research Fund-Biosciences Research Infrastructure Fund's joint competition, which will be followed by other relevant NSERC research partnership programs that were not included in the pilot phase. The expanded application of the *Guidelines* will continue to be conducted in phases, and at a later date, they will also be implemented at CIHR, followed by SSHRC. The expansion of the application of the *Guidelines* is supported by $159.6 million in funding, starting in 2022-2023, and $33.4 million ongoing, that was announced in Budget 2022, which will provide direct financial support to eligible institutions and towards the establishment of the Research Security Centre. Further details will be announced by each granting agency as the relevant funding opportunities are launched.

Given that the threats to research are increasing, in a Statement published on February 14, 2023, we announced that the federal research granting agencies and CFI must adopt a new research security posture in addition to the existing National Security Guidelines for Research Partnerships. As such, grant applications that involve conducting research in a sensitive research area will not be funded if any of the researchers working on the project are affiliated with a university, research institute or laboratory connected to military, national defence or state security entities of foreign state actors that pose a risk to our national security. This new action will further strengthen the country's research security posture while continuing to support an open and collaborative research enterprise.

We encourage all researchers engaging in research partnerships to familiarize themselves with the new Statement and *Guidelines* to learn more about implementing voluntary research security due diligence practices. Researchers can visit the *Safeguarding Your Research* portal to access the free research security training courses and guidance on conducting open source due diligence. These resources, among others, will help to ensure a better understanding of Canada's overarching research security framework.

The Honourable
François-Philippe
Champagne,
Minister of Innovation,
Science and Industry

The Honourable
Dominic LeBlanc,
Minister of Public Safety

The Honourable
Mark Holland,
Minister of Health

1. Introduction

Purpose and scope of the Progress Report

Innovation, Science and Economic Development Canada, Public Safety Canada, and Health Canada are pleased to share this Progress Report on the implementation of Canada's National Security Guidelines for Research Partnerships (the *Guidelines*) and supporting research security efforts. This publication includes information on the results of the pilot implementation of the *Guidelines* in NSERC's Alliance program, and highlights other initiatives that are underway to safeguard Canadian science, data, and research.

Canada's research ecosystem is open, inclusive, and collaborative

Canada is at the forefront of science and research, and our country continues to foster a growing and dynamic knowledge-based economy. Canada's research ecosystem embraces creativity, discovery, and innovation, which is enabled by open science principles.

In turn, open science is supported by people, technology, and infrastructure, and is practiced through respecting privacy, expanding security and ethical considerations, and adopting appropriate intellectual property protections. The Government of Canada's commitment to these practices is demonstrated through the adoption of the *Roadmap for Open Science* to ensure that research and science is accessible to all, and is sustainable, transparent, collaborative, and inclusive.

Canada's commitment to open science attracts national and international research partners, and these collaborations provide Canada with the capacity to contribute and benefit from the economic, environmental, and social benefits of world-class research. Due to the advanced nature of Canada's research ecosystem, Canadian-led research can also be an attractive target for those who seek to use any and all means to acquire this research, knowledge, and data for their own priorities and gains.

Canada's approach to furthering innovation and safeguarding research follows the principles of Equity, Diversity, and Inclusion (EDI). Freedom from discrimination is a fundamental and internationally recognized human right that is necessary for all aspects of the research enterprise. Supporting EDI is essential to creating the excellent, innovative, and impactful research necessary to advance knowledge and understanding, and to respond to local, national, and global challenges. In line with these commitments and principles, the Government of Canada acknowledges that threats can come from any country and has adopted a country-agnostic approach. Our framework also strives to guard against any conscious and unconscious biases that could result in discriminatory behaviors or decisions.

The Government of Canada will continue to support and work with domestic and international research communities to safeguard Canadian research, while also upholding these shared commitments to open science and EDI.

Open science and research security are complementary and mutually reinforcing

Security and openness are not mutually exclusive. Rather, they can both contribute towards ensuring trust, integrity, and mutual reciprocity in a collaborative and open research ecosystem. The Government of Canada seeks to advance the foundational principles and freedoms of academic research in tandem with the need to safeguard Canada's world-leading research ecosystem to ensure that publicly-funded research maximizes benefits for Canada and Canadians, now and into the future.

In May 2020, the Canadian Security Intelligence Service (CSIS) issued a joint Statement with the Communications Security Establishment (CSE) warning researchers in the life sciences sector of increased targeting towards Canadian COVID-19 research by foreign intelligence services. Later, in February 2021, CSIS expanded on these emerging threats, noting that additional research areas are at risk given that the geopolitical threat landscape is evolving and increasing in complexity. Of particular concern is that Canadian knowledge and expertise can be leveraged by foreign governments and organizations for human rights infringements, and commercial, economic, or military gain, without the knowledge or authorization of those conducting and funding the research.

In September 2020, the Ministers of Public Safety, Health, and Innovation, Science and Industry, announced that research related to COVID-19 was experiencing a higher volume of threats from foreign hostile actors. This Statement encouraged researchers in the health sector to take extra precautions to protect their research, intellectual property, and knowledge development. An additional announcement was made in spring 2021, emphasizing that all areas of research are increasingly at risk due to Canada's reliance on digital infrastructure and the prevalence of cyber threats. In response to this concern, the Minister of Innovation, Science, and Industry, the Minister of Public Safety, and the Minister of Health, announced the intent to integrate national security considerations into the development, evaluation, and funding of research partnerships.

Completion of the pilot phase for the National Security Guidelines for Research Partnerships

The *Guidelines* were developed and published in July 2021 by the Government of Canada, in consultation with universities and associations that represent academic institutions. This policy framework identifies important national security considerations for all members of the Canadian research community – including, but not limited to, researchers, academic institutions, and research funders – who support or participate in research projects with partner organizations.

A key component of the *Guidelines* is 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).

To pilot the integration of national security considerations into the development, evaluation, and funding of research partnerships, the *Guidelines* were applied on a mandatory basis in the first phase to NSERC's Alliance grants program, recognizing that this program funds research in sensitive areas that may carry higher security risks. Beyond their implementation into federal research funding programs, such as Alliance, the due diligence approach and methodology that is supported by the *Guidelines* and the Risk Assessment Form can also be applied by anyone in the Canadian research community to identify and mitigate risks within their research partnership projects.

2. Importance of Research Security and Efforts to Enhance it in the Canadian Research Ecosystem

Research security safeguards scientific research

The concept of research security encompasses the set of actions that can identify and protect our research community from actors and behaviours that pose national and international security risks. For example, these risks can include undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal actors; and other activities and behaviours that have adverse national security implications.

Canada is committed to building a robust research security culture, by promoting due diligence efforts, open dialogue, and adopting risk mitigation practices. 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 aims to implement research security practices that are **risk-targeted** and **appropriately scaled**, in recognition that research safeguards can have adverse impacts on innovation, partnerships, research communities, and the advancement of mutually beneficial research, and that the likelihood of a risk occurring and the significance or magnitude of a breach can vary. Through proactive research security practices, the government, researchers, academic institutions, and funders can work together to identify, assess, and mitigate these risks and protect the inputs, processes, and products that are part of scientific research and discovery – in a way that takes into account both the aggregate level of risk and the potential impacts to innovation and mutually beneficial research. In doing so, research security practices can enhance risk awareness among researchers, and can reinforce the foundations of academic freedom, scientific openness, transparency, and trusted collaborations for mutual benefit.

Canada's research security approach is country and company agnostic, based on the recognition that threats evolve and can originate from anywhere in the world. In response to the constantly evolving threat environment, Canada has put forward several initiatives that safeguard and protect the Canadian research ecosystem.

Research security is a shared responsibility

Research security is a collective effort – researchers, research institutions, funding organizations, and governments have a shared responsibility to identify and mitigate any potential national security risks related to research. The *Guidelines* are one element of a multi-pronged approach to enhance Canada's research security capacity. They provide a framework that researchers and research institutions can follow to conduct consistent, and risk-targeted due diligence to improve their research security posture as it relates to research partnerships.

Furthermore, the *Guidelines* are designed to be implemented as a requirement for federal research partnership funding programs, wherein they provide a mechanism for Canada's research funding organizations and national security departments and agencies to assist in the appropriate identification and mitigation of risks for certain projects and collaborations.

The *Guidelines* build on and are complemented by the following initiatives, which are already in place to help the research community implement research security considerations into their practices:

- The *Safeguarding Science* initiative was launched in 2016 by Public Safety Canada (PSC) through a collaborative partnership involving several federal departments and agencies. This initiative offers workshops to the Canadian research and academic community and provides a broad overview of research security threats and mitigation strategies.
- The *Safeguarding Your Research* portal was launched in 2020 by Innovation, Science and Economic Development Canada (ISED). It was developed in collaboration with several federal departments and agencies and was informed by the research community. This platform is updated regularly with new guidance and resources to provide useful information to the Canadian research community on how to safeguard their research and assets, including tools such as: training courses, briefing videos, checklists, detailed guides, case studies, and interactive activities.

Federal resources such as the *Safeguarding Science* initiative, the *Safeguarding Your Research* portal*,* and the *Guidelines*, are Government of Canada tools that individuals can collectively harness to assess and mitigate security risks to their research – even if they are not seeking federal funding for their research.

3. Canadian Progress in Enhancing Research Security

The federal government is taking concrete measures to protect cutting-edge Canadian research, development, data, and technology, that is being actively targeted by foreign state actors to advance their geopolitical, economic, and security interests. In addition, the Government of Canada also continues to work closely with the academic research sector, private sector organizations, as well as our international allies, to develop policies and practices to protect research. Through these collaborations at the national and international level, Canada has been able to contribute to the development of global research security standards while advancing an approach to research security that is holistic and can adapt to an ever-changing threat landscape. These efforts also strive to support a fair and equitable global research ecosystem that enables collaborative research between Canadian and international researchers.

The Government of Canada is building research security tools and resources

The *Safeguarding Your Research* portal was developed with input from the academic community and is the Government of Canada's main public resource to raise awareness about research security. It provides information on best practices and guidance on how to identify and mitigate potential national security risks in research and science, and includes links to other relevant domestic and international content.

Several new resources were added to the *Safeguarding Your Research* portal in 2022, including:

- An Open Source Due Diligence Guide to help researchers conduct due diligence regarding their partners based on open sources of information.
- Two informative videos "Why safeguard your research?" presented by the Chief Science Advisor of Canada, and "Why the Guidelines?" presented by the President of NSERC.
- A Frequently Asked Questions webpage that helps direct researchers to the information needed when completing the Risk Assessment Form associated with the National Security Guidelines for Research Partnerships.

Budget 2022 announced additional efforts that will support Canada's implementation of the *Guidelines*. These include the establishment of a Research Security Centre as well as funding through the Research Support Fund for eligible post-secondary institutions to build their research security capacity, starting in 2023.

Continuous engagement with Canada's research community

Since 2016, PSC has been leading the *Safeguarding Science* initiative to provide interactive workshops to Canadian universities and the broader research community to equip them with the knowledge and tools required to protect their valuable research. In the midst of the pandemic, PSC continued to engage with Canada's research community to raise awareness of research security issues through the *Safeguarding Science* initiative. This was accomplished by delivering workshops to stakeholders, virtually rather than in-person. This change supported the continuous delivery of the workshops during a time when the risks to research security were heightened. As a result, the initiative nearly doubled the number of workshops conducted and the number of participants who received a workshop, as compared to the previous year. In 2021, workshops were delivered to twelve academic institutions and eight research institutions, reaching a total of 1,398 participants. Since its inception in 2016, the program has reached 51 academic institutions, 31 research institutions, and 23 other federal departments and agencies.

Furthermore, 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 of guidance documents and other information resources. In 2022, CSIS' Academic Outreach and Stakeholder Engagement program held 42 meetings on this topic, with 35 organizations across Canada.

This outreach to academia is complemented by the Government of Canada-Universities Working Group, a key governance mechanism, which was established in 2018 to collaboratively identify, share, and promote best practices to mitigate security risks, protect data and intellectual property. The group meets regularly and continues to develop resources, as appropriate, in response to emerging issues across the Canadian research ecosystem.

In addition, since the publication of the *Guidelines* in summer 2021, ISED, NSERC, and PSC have held several information sessions and participated in a number of events and webinars to promote awareness on research security and to provide detailed information to aid researchers and institutions in complying with the *Guidelines*.

Collaborating with international partners on research security best practices

At the international level, Canada continues to work closely with allied countries and various organizations to develop an evidence-informed and comprehensive strategy to research security. Since 2021, the Government of Canada, with participation from Canadian academic community representatives, has engaged on the topic of research security with allies, and likeminded countries, through various international groups and forums.

Notably, Canada's 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.

Represented by ISED, Canada is Co-Chair of the G7's Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE). This working group was established as a result of the G7 Research Compact, signed in summer 2021, which committed all members of the

G7 to advancing shared research security priorities and established the Working Group. The SIGRE Working Group aims to:

- Establish a list of principles that underpin secure and mutually beneficial research;
- Produce a list of best practices that organizations can take to improve their research security posture; and
- Pool together research security resources to launch an online Virtual Academy and toolkit that will share tools and training.

In June 2022, the SIGRE working group achieved its first objective through the publication of the *G7 Common Values and Principles on Research Security and Research Integrity*.

ISED also led the Government of Canada's contributions to the OECD Global Science Forum's research security and integrity report titled *Integrity and security in the global research ecosystem*. This report, also published in June 2022, profiles Canadian and international approaches to research security and offers policy recommendations for others looking to advance efforts in this space.

In addition, Global Affairs Canada leads 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.

In recent years, Canada's efforts to advance international research security have enabled significant opportunities for future information sharing and coordinated approaches among allies, so that we can all benefit from a shared, secure approach. The Government of Canada will continue to participate and lead in these meaningful dialogues, workshops, and multilateral fora that look to address research security.

4. Implementation of *Guidelines'* Risk Assessment Process into Federal Research Partnership Funding Programs

A risk-based approach

The implementation of the *Guidelines* as a requirement of federal research partnership funding programs adopts a country and company agnostic framework. The implementation of the *Guidelines* began with the NSERC Alliance grants program where a private sector partner was involved, recognizing that this program funds projects in a sensitive research area that can carry higher national security risks.

Risk assessment process overview

An integral component of the risk assessment process is the Risk Assessment Form. Researchers complete the form by conducting open-source due diligence, by working with internal resources and services within their institutions, and by consulting with their partner organization(s), where appropriate, to validate their responses. Following that, the completed form is submitted alongside their research partnership grant application. As with all other application documentation and information that is provided by the applicant, the Risk Assessment Form is only used for its intended purpose – to collect information on and assess risks related to the research partnership.

For each research partnership application submitted with a Risk Assessment Form, the risk assessment process is conducted in three steps:

Step 1: Administrative validation by the granting agency

First, the Risk Assessment Form is administratively reviewed by the granting agency to ensure that all the questions and components on the form have been completed by the applicant. This review also includes a risk validation assessment using open-source due diligence methods, based on the risk factors outlined in the *Guidelines*. As part of the administrative review process, applications with possible or identified risks are referred to the granting agency's internal Risk Assessment Committee, which discusses each application on a case-by-case basis and determines whether additional assessment and advice is required from the national security departments and agencies.

Applications that are deemed complete proceed to merit assessment using the granting agency's established mechanisms of peer review. The Risk Assessment Form is not shared with peer reviewers.

In cases where the granting agency's internal risk assessment identifies a need for a national security assessment and advice to inform the funding decision, the relevant application documents are referred to PSC. This referral usually occurs after the merit assessment has been deemed successful, but prior to a funding decision being rendered by the granting agency.

Step 2: Referral of applications to Public Safety Canada

PSC coordinates national security-related activities across relevant federal departments and agencies. The department's mandate is to keep Canadians safe from a range of risks such as natural disasters, crime, and terrorism. As part of PSC's mandate, the Minister of Public Safety is responsible for policy leadership in the areas of national security and economic-based threats to national security. This includes leading the coordination of the federal security and intelligence community in safeguarding Canada's world-leading research ecosystem, as well as intellectual property businesses.

Upon receipt of a funding application from a granting agency, PSC conducts an initial review to determine which security agency is responsible for leading the national security assessment of the proposed research partnership project. The lead security agency may be Public Safety Canada (PSC), the Canadian Security Intelligence Service (CSIS), or the Communications Security Establishment (CSE).

- **Canadian Security Intelligence Service (CSIS)** is an intelligence agency that investigates and advises on activities suspected of constituting a threat to the security of Canada, and takes measures to reduce such threats. CSIS's priorities include threats that can jeopardize the safety and prosperity of Canadians and Canada's economic, national, and research security.

- **Communications Security Establishment (CSE)** is the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance.

The lead security agency, under their respective authorities and mandate, conducts a national security assessment and provides it to PSC. PSC may further consult other relevant departments such as Global Affairs Canada to take into account other relevant considerations related to the science, economic benefits, or global implications of the funding application, to inform its assessment results and advice that is returned to the granting agency.

Step 3: Funding decision

The granting agency considers the national security assessment and advice received from PSC, alongside the result of the merit assessment, to make a funding decision for each application. The granting agency then notifies the applicant of its funding decision.

The applicant is provided a decision letter that includes information on the results of the merit assessment and information on the national security assessment of their application (where applicable). The Government of Canada is committed to ensuring transparency across all funding decisions while also building the science and research community's level of risk awareness. Where applicable, applicants that were denied funding will be offered the opportunity to request a meeting with representatives from the respective granting agency and the Research Security Centre to discuss the results of their application's national security assessment.

If an applicant receives funding for their proposed research project, they must implement the risk mitigation plan outlined in their application for the duration of the project. Dependent on the advice provided by the national security departments and agencies, the granting agency may require the implementation of additional mitigation measures as a condition of funding.

5. Tracking the Impact of Canada's National Security Guidelines for Research Partnerships

Key results from the National Security Guidelines for Research Partnerships pilot phase

Between July 23, 2021 and July 23, 2022, NSERC received a total of 1158 research partnership applications that required a Risk Assessment Form, under the Alliance grants program and the Alliance Missions special call.

NSERC's administrative risk validation process added on average 1-2 business days to the processing time of Alliance applications. Most applications (~96%) were cleared by NSERC at this stage, and therefore program service standards were maintained. Approximately 4% of applications required further national security assessment and advice from the national security departments and agencies.

Analysis of responses to questions on the Risk Assessment Form

Most applicants (92.6%) were found to have thoroughly completed the Risk Assessment Form. In addition, many applicants also provided detailed answers to the questions on the Risk Assessment Form, thereby demonstrating a strong understanding of potential risks to their research. The quality of the responses illustrates that applicants have made a best effort to assess the security risks associated with their research project and private sector partner organization(s), and have developed appropriate mitigation plans.

The results of the administrative risk validation conducted by NSERC were consistent with most of the responses submitted by applicants on the Risk Assessment Form. However, NSERC identified that applicants faced challenges with some questions from the "Know Your Partner Organization" section of the Risk Assessment Form, including three questions pertaining to identifying affiliations, government influence/control, and criminal history. For these questions, approximately 35% of applicants reported "no risk", while the administrative risk validation conducted by NSERC resulted in an "unsure" response.

This demonstrated that further guidance is required on how to respond to questions that require open source due diligence methods and knowledge of the geopolitical landscape. This guidance has been developed and is now available on the *Safeguarding Your Research* portal, since November 2022: see Conducting Open Source Due Diligence for Safeguarding Research Partnerships.

Summarizing the results of the National Security Guidelines for Research Partnerships pilot phase in NSERC's Alliance Grants program

1110 applications (~96% of the 1158 applications) that were processed through NSERC's administrative risk validation process did not require further national security assessment. Of these 1110 applications, 86 applications (7.7%) were rejected because of an incomplete Risk Assessment Form, while 139 applications (12.5%) were rejected for administrative reasons unrelated to the *Guidelines*. Among these, 664 applications (59.8%) were funded while 213 (19.2%) were not awarded based on the results of the merit assessment. 5 applications (0.5%) were withdrawn by the applicant, while 3 applications (0.3%) remain under merit assessment.

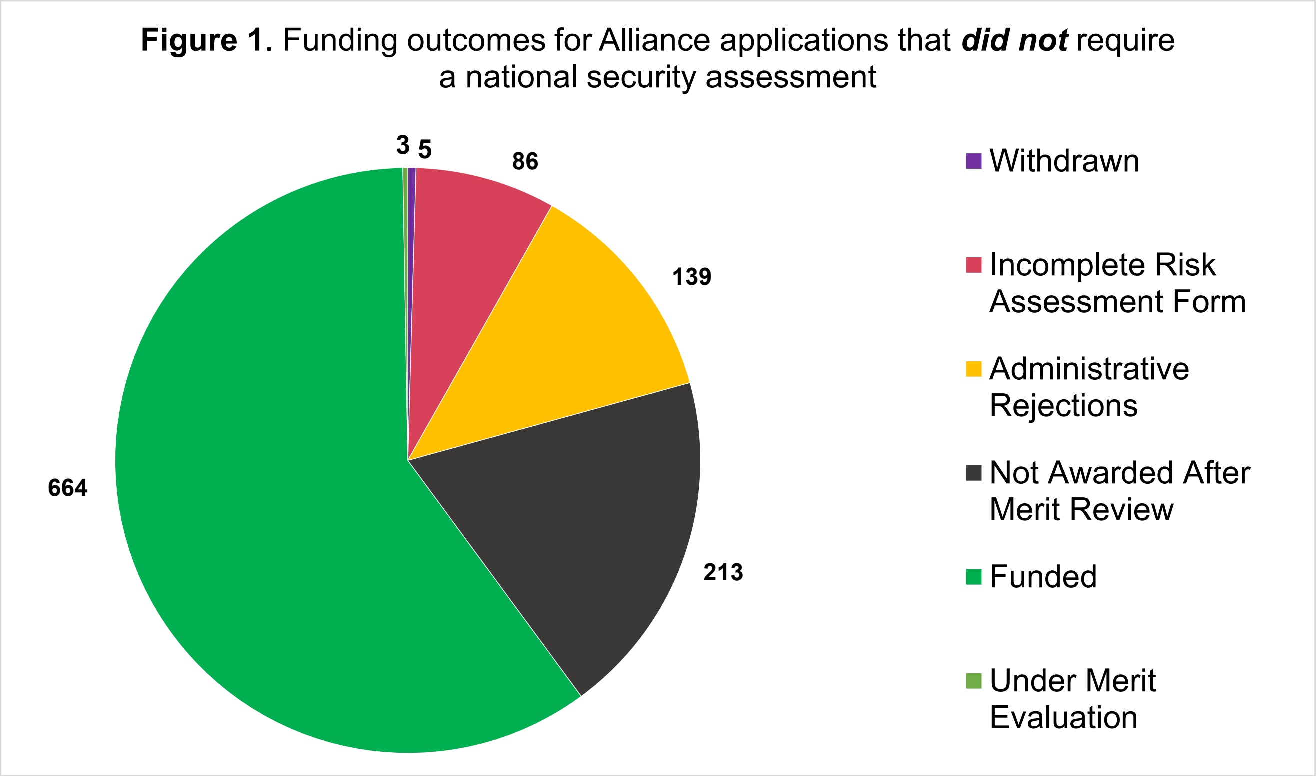

Figure 1. Funding outcomes for Alliance applications that did not require a national security assessment. *The chart provides a visual representation of the breakdown of the different funding outcomes based on NSERC's initial administrative validation of Alliance program applications between July 2021 and July 2022.*

In all, 48 applications (~4% of all applications) were referred for a national security assessment between July 2021 and July 2022.

Of the 48 applications referred for a national security assessment:

In 13 cases, NSERC was advised by PSC that the research partnership proposed in the application should not pose a risk to Canadian national security. In one additional case, NSERC was advised that the mitigation plan proposed by the applicant was insufficient to mitigate the risks identified; additional mitigation strategies were therefore provided to the applicant, to be implemented as a condition of their award. These 14 applications were found to be meritorious, through NSERC's merit assessment process and were awarded funding.

In 2 cases, the applicant withdrew their application prior to NSERC rendering its funding decision; therefore, no decision letter was provided to the applicants. In 32 cases, NSERC was advised by PSC that the research partnership proposed in the application poses an unmitigable risk to Canadian national security. The *Guidelines* state that applications for partnerships that are assessed to present an unacceptable risk to national security and/or where risks cannot be appropriately mitigated, will not be funded. As a result, these applications were not awarded funding by NSERC.

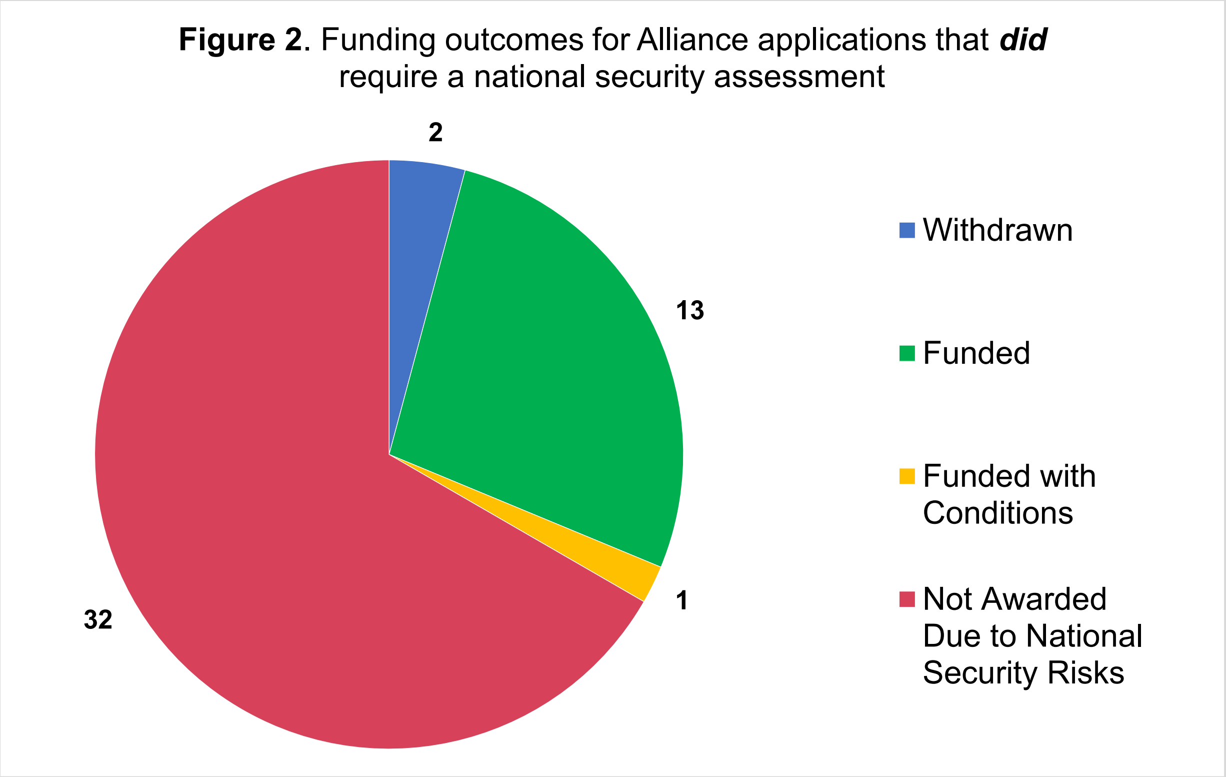

Figure 2. Funding outcomes for Alliance applications that did require a national security assessment. *The chart provides a visual representation of the funding results only for NSERC Alliance applications that required a national security assessment following NSERC's initial administrative validation process conducted between July 2021 and July 2022. The findings displayed in this visual are organized based on four possible outcomes: funded, funded with conditions, not awarded due to national security risks, and application withdrawn before funding decisions were announced.*

NSERC and the national security departments and agencies noted a set of common risk factors that were present among the applications not funded as a result of the national security assessment process. To date, these factors relate to private sector partner organizations that were found to have:

- Public ties to foreign states known to target academic institutions, the private sector, and the general public; and/or
- A public record of not complying with import/export regimes.

While these risk factors were related to publicly accessible information, the Risk Assessment Forms completed by applicants often did not include this information. This supports the need for guidance on open source due diligence methods among the research community.

Impact of the *Guidelines* on the Alliance program and its diversity of applicants and partner organizations

Throughout the pilot phase of implementation of the *Guidelines*, NSERC and other Government of Canada departments have monitored key data and continue to be vigilant of any potential unintended consequences for the Alliance program and the research community.

To date, the *Guidelines* were found to have no impact on the diversity of applicants who receive funding from the Alliance program. This is reflected in the application success rates, which have remained consistent including for applicants who self-identified as a visible minority:

Visible minority status	**Yes**	**No**	**Prefer not to answer**
Success rate* June 2019 – June 2021 (pre-*Guidelines*)	80%	82%	83%
Success rate* July 2021 – July 2022 (post-*Guidelines*)	85%	86%	88%

* *Not including rejected applications.*

The *Guidelines* have also had a negligible impact on the diversity of partners that are involved in projects that receive funding through the Alliance program. This is reflected by consistency in the percentage of partners from the private, public, and not-for-profit sectors that participate in funded research projects, as there was not a significant shift in applications favouring public or not for profit partners over private sector partners:

Participation by partner sector	**Private**	**Public**	**Not for Profit**
June 2019 – June 2021 (pre-*Guidelines*)	66%	19%	16%
July 2021 – July 2022 (post-*Guidelines*)	64%	18%	18%

These outcomes indicate that the implementation of the *Guidelines* in the Alliance program have had an overall minor impact on the diversity of applicants and partner organizations.

Delays in the assessment of applications during the pilot phase of the National Security Guidelines for Research Partnerships

The government has worked diligently since July 2021 to develop the processes and procedures to implement the *Guidelines* into the evaluation and funding of grant applications in a manner that protects the applicant's information to the same standard that researchers expect when providing their Alliance applications to NSERC for merit review.

Given the time required to develop and refine this process, the 4% of applications that required a national security assessment were subject to exceptional delays. The Government of Canada recognizes the significant impact that delays in funding decisions can cause, not only for the applicant(s) and their research team, but also for the viability of the proposed partnership projects. As the implementation of the *Guidelines* continues to be refined, clear service standards for this process will be developed and communicated as the Government of Canada remains committed to completing these assessments in a timely manner while upholding the quality and rigour of the analysis.

These assessments will continue to enhance the central objectives of research partnership funding programs, such as Alliance, to support research projects led by strong, complementary, and collaborative teams across sectors, to generate new knowledge while accelerating the application of research results to create benefits for Canada.

6. Feedback from the Research Community

A number of consultation exercises, including surveys, outreach presentations, and working group discussions were undertaken during the pilot phase, to gather feedback from the research community. This feedback can be grouped into three overarching areas of improvement.

Researchers want help identifying risks within their research projects and partnerships

Feedback received during the pilot phase suggests that the research community is continuing to build its awareness and capacity to identify risks, and that varying levels of awareness exist across the research community. More specifically, the research community has expressed difficulty in understanding if their research could be of interest to foreign governments or militaries, or if their partner organizations may have affiliations that could lead to the transfer of research to third party governments, militaries, or organizations that could negatively impact Canada's national security. They have also raised concerns about how the implementation of research security due diligence may impact their pre-existing relationships with partner organizations.

Researchers and institutions want more resources and guidance, especially to help identify risk mitigations

The input received throughout the pilot phase suggests that the research community continues to seek additional resources and guidance from the Government of Canada. They are particularly interested in guidance that focuses on how to identify and implement appropriate risk mitigations to ensure that research partnerships can proceed and continue to be supported. To access this guidance, many individuals from the academic community indicated their preference for a clear first point of contact within the Government of Canada to coordinate and engage on all research security matters. The feedback received notes that, while some risk mitigations can be implemented at the project level, some research security risk mitigations need to be implemented at the institutional/organizational level. For example, while researchers recognize the importance of cybersecurity measures, it was acknowledged that cybersecurity measures are most often implemented by institutions rather than by individual researchers, and therefore it is beyond the capability of the researcher to commit to such measures in their individual risk mitigation plans.

While the feedback indicates that several institutions have begun to put in place institutional-level processes and tools to help their researchers integrate risk mitigation measures, this could be bolstered through additional guidance tailored both to the institutional and project level.

Respondents recommended changes to the Risk Assessment Form

Given that the pilot phase of the *Guidelines* marked the first use of the Risk Assessment Form, several researchers, administrators, and institutions provided suggestions on how the questionnaire could be improved.

Many noted that by removing some questions and using a streamlined Risk Assessment Form, would increase its usability and level of ease. In addition, general feedback suggested maintaining the use of a standardized questionnaire for all relevant federal funding opportunities subject to the future roll-out of the application of the *Guidelines*.

7. 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.

The Government of Canada recognizes that this is a new concept to many in the Canadian research ecosystem, and that further work will be required to ensure that all parties involved – researchers, research institutions, granting agencies, and federal departments – have the knowledge and tools to apply new research security requirements such as the *Guidelines*.

The Government of Canada is committed to working closely with all members of the research ecosystem to implement targeted safeguards that are specific to the risks that emerge within the field of science, that also allow for open and collaborative science to continue, while ensuring that researchers’ knowledge, data, and intellectual property are protected.

Budget 2022 proposed a package of research security measures

To implement the *Guidelines* fully, Budget 2022 committed to provide $159.6 million, starting in 2022-2023, and $33.4 million ongoing, as follows:

- $125 million over five years, starting in 2022-2023, and $25 million ongoing, for the Research Support Fund to build capacity within post secondary institutions to identify, assess, and mitigate potential risks to research security; and
- $34.6 million over five years, starting in 2022-2023, and $8.4 million ongoing, to enhance Canada's ability to protect our research, and to establish a Research Security Centre within the federal government.

The Research Security Centre is operational and has been staffed with regional advisors throughout summer 2023. The Research Security Centre provides advice and outreach to the research community, through workshops and other tools. This includes coordinating across the federal government to ensure outreach, awareness, and threat briefings to complement existing activities. Investments to build research security capacity within post-secondary institutions through the Research Support Fund began in 2023.

Additional guidance and tools will continue to be developed and added to the *Safeguarding Your Research* portal, including resources that are tailored to provide guidance on developing appropriate risk mitigation measures.

The above initiatives will support the future roll-out of the *Guidelines.* The expanded roll-out began in early 2023 with the Canada Biomedical Research Fund-Biosciences Research Infrastructure Fund's joint competition, which will be followed by other relevant NSERC research partnership programs that were not included in the pilot phase. The expanded application of the *Guidelines* will continue to be conducted in phases, and at a later date, they will also be implemented at the Canadian Institutes of Health Research and the Social Sciences and Humanities Research Council. Additional research funding programs may apply the *Guidelines*, or integrate other research security measures, as they launch programs or calls for proposals, based on the nature of their program and the related risks.

Further implementation of the *Guidelines* will be informed by lessons learned from the pilot implementation in NSERC's Alliance grants program. Additional details will be announced by each granting agency as the relevant funding opportunities are launched.

To support the future roll-out of the *Guidelines*, the Risk Assessment Form has been updated. The update reflects input that was received from researchers, institutions, and input from implicated government departments and agencies, to ensure that the questions are more straightforward, streamlined, and targeted.

Strategy for measuring the future success of the *Guidelines*

The Government of Canada has developed a performance measurement strategy to monitor and assess the results and outcomes of the implementation of the *Guidelines*.

This strategy includes tracking the achievement of the following objectives:

- The availability of information and tools that help to safeguard research;
- An increase in research security and risk awareness among academic institutions;
- The identification of potential research partnership risks and mitigation measures;
- The systematic application of risk-proportionate due diligence that avoids unintended consequences;
- A reduction in the national security risks associated with federally-funded research partnerships; and
- The integration of research security into Canada's research and innovation culture.

To implement this performance measurement strategy – for the NSERC Alliance program as well as future funding programs – data will be collected starting in 2023-2024, including through an annual online Research Security Survey. This survey will be sent to academic institutions across the country encouraging research administrators, legal services, and researchers, to complete the questionnaire. The results of this performance assessment, including key takeaways from the survey, will be reported in future reports on the implementation and progress of the *Guidelines.*

Continuing to work together to safeguard research

Given that the threat environment is constantly evolving, a ministerial Statement was released on February 14, 2023 by the Ministers of Innovation, Science, and Industry, Health and Public Safety, and requested that the Canada Foundation for Innovation and Canada's tri-agency granting councils adopt an enhanced posture regarding national security. This new posture states that grant applications seeking to conduct research in a sensitive research area will not be funded if any of the researchers working on the project are affiliated with a university, research institute or laboratory connected to military, national defence or state security entities of foreign state actors that pose a risk to our national security.

The implementation strategy for this policy was developed in close consultation with federal departments, granting agencies, Canada's national security agencies, and the research community. For more information on the requirements and application of this new ministerial directive, as well as resources that support its implementation, please consult the fall 2023 follow-up policy Statement.

Ultimately, all of Canada's research security measures – including the *Guidelines* — are designed and intended to better safeguard Canadian research, intellectual property, data, and knowledge development. These measures aim to preserve the 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.

The effective integration of research security due diligence is an evolving process for all members of the Canadian research community – including funding organizations, academic institutions, and researchers. The Government of Canada recognizes that research security is a new concept for some in the research community, and is committed to maintaining open and transparent dialogue as we collectively continue to safeguard Canadian research, data, and technology.