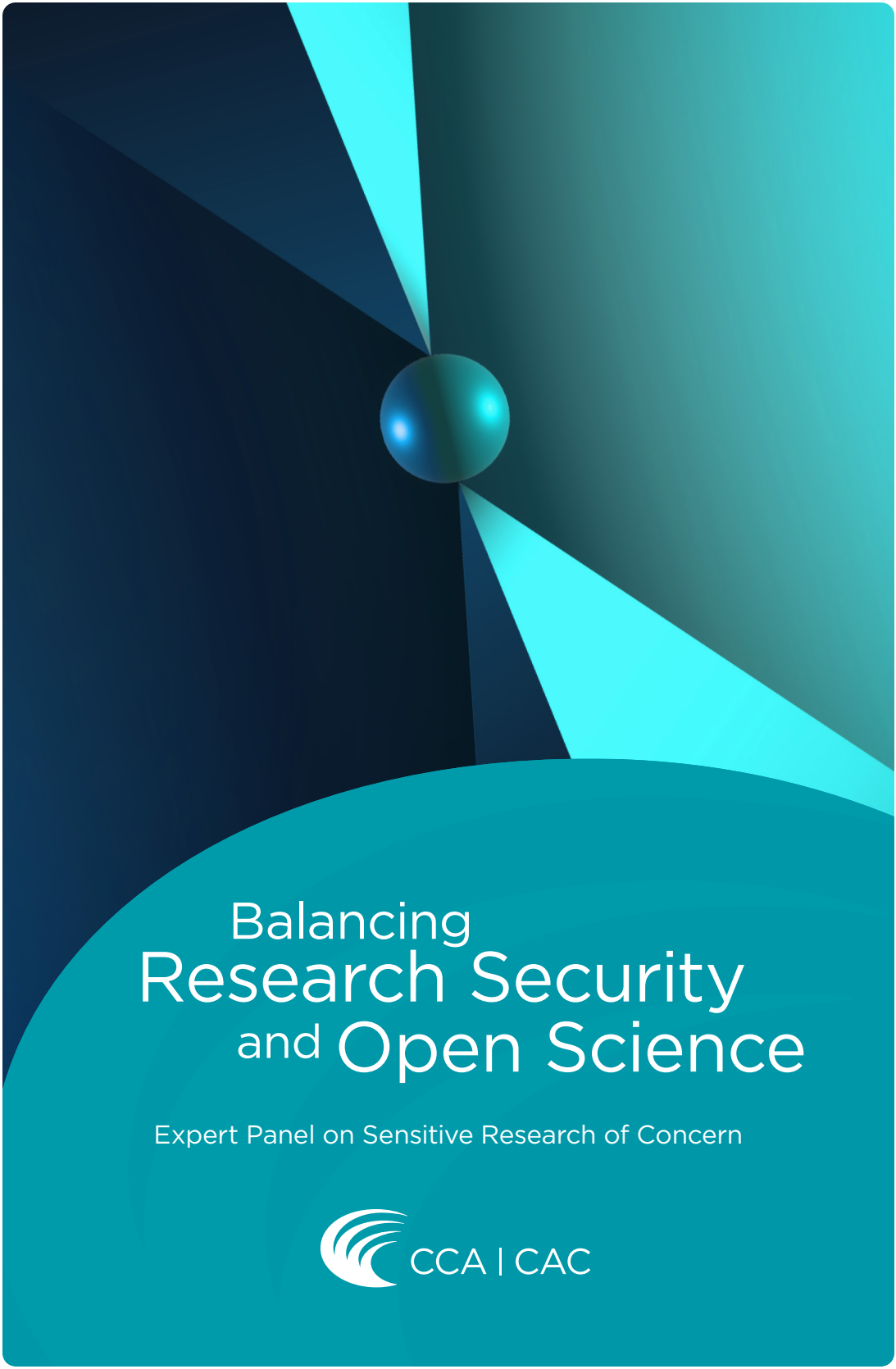


# Balancing Research Security and Open Science

Expert Panel on Sensitive Research of Concern

CCA | CAC

# Balancing Research Security and Open Science

Expert Panel on Sensitive Research of Concern

COUNCIL OF CANADIAN ACADEMIES
180 Elgin Street, Suite 1401, Ottawa, ON, Canada, K2P 2K3

This project was undertaken with the approval of the Board of Directors of the Council of Canadian Academies (CCA) and responds to a request from the sponsors, Defence Research and Development Canada (DRDC) and the Public Health Agency of Canada (PHAC) for an independent assessment. The sponsors were not involved in either panel selection or report development; any opinions, findings, or conclusions expressed in this publication are those of the authors, the Expert Panel on Sensitive Research of Concern, and do not necessarily represent the views of their organizations of affiliation or employment.

## Suggested citation:

CCA (Council of Canadian Academies). (2025). *Balancing Research Security and Open Science.* Ottawa, ON: Expert Panel on Sensitive Research of Concern, CCA. https://doi.org/10.60870/fmt9-9559.

ISBN: 978-1-990592-59-1 (Electronic book)
DOI: 10.60870/fmt9-9559

## With assistance from:

| | |
|---|---|
| Cover designer | Ryan Hook, Atiigo Media |
| Editor | Jody Cooper |
| Layout and design | Atiigo Media |
| Translator, En-Fr | Dany Gagnon and Anne-Marie Mesa |

## Disclaimer:

Reference made in this report to any specific company, commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute its endorsement, recommendation, or favouring.



This project was made possible with the support of the Government of Canada through the Strategic Science Fund.

The Council of Canadian Academies (CCA) offices in Ottawa are located on the unceded traditional territory of the Anishinaabe Algonquin People, who have cared for these lands for millennia.

The CCA is committed to reconciliation and honouring Indigenous sovereignty. Through our work in providing evidence for decision-making, we recognize that a wide range of knowledges and experiences contribute to building a more equitable and just society. We encourage all who engage with our work to further learn about and acknowledge the past and present context of the land now known as Canada and of the Indigenous Nations and Peoples who steward it.

# Expert Panel on Sensitive Research of Concern

Expert panel members serve as individuals and do not represent their organizations of affiliation or employment. Each panellist was selected for their expertise, experience, and demonstrated leadership in fields relevant to this project.

**Martha Crago, C.M., PhD, DSc, BVO, (Chair),** Professor and Former Vice President Research and Innovation, McGill University (Montréal, QC)

**Kelly Cobey, PhD,** Director, Metaresearch and Open Science Program, University of Ottawa Heart Institute (Ottawa, ON)

**Jim Ghadbane,** Former President and CEO, CANARIE Inc. (Ottawa, ON)

**Garfield Giff, PhD,** Research Chair, Climate Change Adaptation, Aurora Research Institute (Inuvik, NT)

**Jacqueline Littlewood, MA,** Director, Research Security, University of Alberta (Edmonton, AB)

**Allison M. Macfarlane, PhD,** Professor and Director, School of Public Policy and Global Affairs, The University of British Columbia (Vancouver, BC)

**Rebecca Moritz, MS, CBSP (ABSA), SM (NRCM),** Director, Office of Research Collaboration and Compliance, Office of the Vice President for Research, Colorado State University (Fort Collins, CO)

**Delilah Ofosu-Barko, BMSc. Hons.,** Director, Institute for Better Health Operations, Trillium Health Partners (Mississauga, ON)

**Catherine Olivier, PhD,** Clinical Assistant Professor, Department of Social and Preventive Medicine, School of Public Health, Université de Montréal (Montréal, QC)

**Jocelyn Tremblay,** Former Director General, Science and Engineering, Defence Research and Development Canada (Québec, QC)

**Andrew Van Kessel, PhD,** Director of Research, Vaccine and Infectious Disease Organization (VIDO), University of Saskatchewan (Saskatoon, SK)

**Anya Waite, PhD,** CEO and Scientific Director, Ocean Frontier Institute, Dalhousie University (Halifax, NS)

**Matthew S. Wiseman, PhD,** Assistant Professor, Teaching Stream, Department of History, University of Waterloo (Waterloo, ON)

# Message from the Chair

Canada contributes substantial research output and impact within the global science ecosystem. Aspects of all kinds of research and innovation may be considered sensitive—that is, while intended for beneficial purposes, they may also be used by nefarious actors to harm the public, public health, public safety, and economic and national security. In an era of accelerating innovation and rapidly shifting geopolitical dynamics, the stakes for securing Canada's sensitive research have risen sharply.

Conducting sensitive research is integral to scientific advancement—and, by extension, to Canada's national interests. It holds enormous value for public health, military acumen, Arctic sovereignty, biosecurity, climate resilience, and technological innovation, among many other fields. The challenge before us is not *whether* we should conduct sensitive research, but *how* to do so in ways that are responsible and secure. Our support of open science needs to be considered alongside research security, as it fosters discovery, accelerates innovation, and enables knowledge-sharing. To that end, securing sensitive research requires thoughtful and adaptive safeguards. These must be calibrated to the risk of the research at hand, implemented throughout the research lifecycle, and grounded in evidence-based policy. Research security should not come at the expense of scientific advancement; it should facilitate trust and the long-term sustainability of the ecosystem itself.

Research security requires shared responsibility across the research ecosystem—from individual researchers and institutional leaders to funding agencies, government departments, intelligence bodies, and the private sector. Each plays a critical role in recognizing, assessing, and mitigating potential misuse of research. Clarity around roles, responsibilities, and expectations is essential to fostering a culture of security that is aligned with a commitment to open science.

Canada is well-positioned to lead in developing and championing models of research security that protect national interests and the global scientific ecosystem while encouraging responsible sharing. By investing in education, training, and capacity-building that acknowledge our diverse research environments—including the rights of First Nations, Inuit, and Métis Peoples over research affecting their communities—we can build a research ecosystem in which openness and security are mutually supportive values.

The terrain of sensitive research is complex. I commend my fellow panellists for navigating it with care. Their expertise, insights, and dedication

demonstrate a deep commitment to securing a robust future for research in Canada—one in which knowledge advances responsibly, ethically, and safely. It has been a pleasure to serve as chair of this panel. I would like to thank my fellow panel members for their contributions and thoughtful deliberations throughout the process, and the CCA team for their support. Finally, I would like to thank Defence and Research Development Canada and the Public Health Agency of Canada for submitting this important question and making our work possible.

**Martha Crago, C.M., PhD, DSc, BVO**
Chair, Expert Panel on Sensitive Research of Concern

## CCA Project Staff

| | |
|---|---|
| Assessment team: | **Anita Melnyk,** Project Director<br>**Anastasia Konina,** Research Associate<br>**Vasa Lukich,** Research Associate<br>**Ananda Fadila,** Project Coordinator |
| Publishing and communications: | **Andrea Hopkins,** Manager of Planning and Production<br>**Brendan Fitzgerald,** Communication Specialist |
| With assistance from: | **Alexei Halpin,** Research Associate<br>**Suzi Loney,** Research Director |

# Peer Reviewers

This report was reviewed in draft form by reviewers selected by the CCA for their diverse perspectives and areas of expertise. Reviewers contributed as individuals and their submissions do not represent the views of their respective organizations. Their anonymized submissions were considered in full by the expert panel. Reviewers were not asked to endorse the conclusions, nor did they see the final draft before its release. Responsibility for the final content of this report rests with the expert panel and the CCA.

**Ingrid d'Hooghe, PhD,** Senior Research Associate, Clingendael Institute (The Hague, the Netherlands)

**Charmaine B. Dean, PhD,** Vice President, Research and International, University of Waterloo (Waterloo, ON)

**Mylène Deschênes, LLB, BCL, LL.M.,** Director, Ethics and Legal Affairs, Fonds de recherche du Québec (Montréal, QC)

**Kenneth M. Evans, PhD,** Scholar in Science and Technology Policy, Baker Institute for Public Policy, Rice University (Houston, TX)

**David Gillum, PhD,** Associate Vice President of Compliance and Research Administration, University of Nevada, Reno (Reno, NV)

**Jennie Knopp, PhD,** Community and Science Director, Oceans North (Ottawa, ON)

**Margaret E. Kosal, PhD,** Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology (Atlanta, GA)

**Matt Malone, LLB, BCL,** Assistant Professor, University of Ottawa Faculty of Law; Director of the Samuelson–Glushko Canadian Internet Policy and Public Interest Clinic (Ottawa, ON)

**Piers D. Millett, PhD,** Executive Director, International Biosecurity and Biosafety Initiative for Science (Geneva, Switzerland)

**David Moher, PhD,** Director, Centre for Journalology, Methodological and Implementation Research Program, Ottawa Hospital Research Institute (Ottawa, ON)

**Kate Moran, O.C., PEng., FCAE, FAAAS, PhD,** President and CEO, Ocean Networks Canada (Victoria, BC)

**Tommy Shih, PhD,** Associate Professor, Lund University (Lund, Sweden)

**Akshay Singh, MA,** Director, Research Security, The University of British Columbia (Vancouver, BC)

The peer review process was monitored on behalf of the CCA by **Benoît Dupont,** Professor, School of Criminology; Canada Research Chair in Cybersecurity and University Research Chair in the Prevention of Cybercrime, Université de Montréal; Scientific Director, Human-Centric Cybersecurity Partnership.

# Acknowledgments

The panel and CCA staff would like to express their sincere appreciation to the following individuals and organizations who shared their knowledge and perspectives:

**Lukas Arenson,** Principal Geotechnical Engineer, BGC Engineering

**David Barclay,** Associate Professor, Department of Oceanography, Dalhousie University

**Rocco Casagrande,** Managing Director, Deloitte

**Sarah-Louise Decrausaz,** Strategic Project Officer, Strategic Research Initiatives, Office of Vice President Research and Innovation, University of Victoria

**Philip Ferguson,** Associate Professor, Department of Mechanical Engineering, University of Manitoba

**First Nations Information Governance Centre (FNIGC)**

**Shayla Fitzsimmons,** Executive Director, Atlantic Regional Association, Canadian Integrated Ocean Observing System (CIOOS)

**Volker Gerdts,** Director and CEO, Vaccine and Infectious Disease Organization (VIDO)

**Government Relations and Policy Research, Colleges and Institutes Canada (CICan)**

**Claire Herbert,** Head of Digital Strategy, Centre for Earth Observation Science, C.H.R. Faculty of Environment, Earth, and Resources, University of Manitoba

**Maia Hoeberechts,** Associate Director, Learning and Community Engagement, Ocean Networks Canada

**Janet King,** Chair, Board of Directors, Polar Knowledge Canada

**Meghan Paulson,** Executive Director, Observatory Operations, Ocean Networks Canada

**Science Policy Branch, Science and Research Sector, Innovation, Science and Economic Development Canada**

**Kanta Subbarao,** Canada Excellence Research Chair in Biology and Control of Zoonotic and Pandemic Respiratory Viruses and Professor, Faculty of Medicine, Université Laval

**Naluturuk Weetaluktuk**

**Dustin Whalen,** Physical Scientist, Geological Survey of Canada, Natural Resources Canada

# Executive Summary

Canada's research ecosystem relies on national, international, and cross-sectoral collaborations to conduct world-class research that offers significant scientific and societal benefits to Canada and its allies. The open and collaborative nature of the Canadian research ecosystem, however, makes it a potential target for malicious state and non-state actors wishing to exploit it to acquire economic, political, technological, or strategic advantages. These potential threats require that those engaged in research are equipped with the necessary tools to identify sensitive research, assess related risks, and adopt measures to safeguard it. A quickly changing geopolitical context, the rapid pace of technological advancement, and the demonstrated interest of a range of actors in misusing or misappropriating Canadian research highlight the need for all participants in Canada's research ecosystem to adopt a proactive and collaborative approach to research security and ensure that research security measures adequately address current and potential threats while balancing open science and innovation.

**Dual-use research of concern (DURC)** is adopted in the life sciences to refer to a subset of dual-use research[1] that, "based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be misapplied to do harm with no, or only minor, modification to pose a significant threat with potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security" (Gov. of United States, 2024a).

**Research security** encompasses a suite of actions and activities intended to identify and protect sensitive research from risks, including but not limited to "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 activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications" (SIGRE, 2022).

(continues)

1 Dual-use research, depending on the context, refers to scientific knowledge, technologies, data, and processes that: (i) have both potential civilian and military applications; or (ii) have the potential for both benevolent and malevolent applications (Kavouras & Charitidis, 2019) and the capacity to do harm on physiological, moral, or ethical grounds (Evans & Commins, 2017).

(continued)

**Sensitive research** refers to the research process and outputs—including but not limited to knowledge, goods, technologies, and data—in a variety of fields that, while intended for beneficial purposes, may be used by nefarious actors or for nefarious purposes to harm the public, public health, public safety, the environment, agriculture, fisheries, sovereignty, and economic and national security in Canada and internationally, or pose privacy and ethics risks (Gov. of New Zealand, 2022; Leopoldina & DFG, 2022a; ISED, 2023a,b; JASON, 2024). The panel acknowledges that this list of potential harms and risks is non-exhaustive and may change depending on the evolving geopolitical context.

**Sensitive research of concern** is a subset of sensitive research that can be reasonably anticipated to be misappropriated or misused immediately or in the future, with no or minimal modifications, and that needs to be subject to additional safeguards (Leopoldina & DFG, 2022a; ISED, 2023a,b; JASON, 2024).[2]

## Open science and research security work together to facilitate the responsible sharing of research

Although open science and research security may be perceived as conflicting priorities because they emphasize different goals, they both inform decisions about when, with whom, to what extent, and in what format research can be shared. Because the level of sensitivity of research may change over time, an ongoing assessment of risks throughout the research lifecycle is necessary to avoid the potential of misuse and oversecuritization. Some types of research may be subject to necessary restrictions on sharing, while others may be openly shared. When research is not subject to restrictions on sharing, its dissemination can help foster transparency, discoveries, and equitable access to information. Concluding that a research type is sensitive and is subject to access restrictions does not mean it should not be funded or carried out. Sensitive research is often of critical importance to innovation, defence, public health, and agriculture, and its findings inform broader scientific advancements. However, to pursue sensitive research projects, researchers and institutions need to minimize the possibility of misuse by developing and adopting appropriate research security measures, including limiting access where appropriate.

2 The definitions of sensitive research and sensitive research of concern were developed by the panel based on the analysis of research security policies and Canada and foreign jurisdictions (CCA, 2025).

**Open science** is a combination of "movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community. It comprises all scientific disciplines and aspects of scholarly practices, including basic and applied sciences, natural and social sciences and the humanities, and it builds on the following key pillars: open scientific knowledge, open science infrastructures, science communication, open engagement of societal actors and open dialogue with other knowledge systems" (UNESCO, 2021). Open science supports collaborative discovery and the reproduction and validation of scientific results.

At the request of Defence Research and Development Canada (DRDC), the Public Health Agency of Canada (PHAC), and other supporting departments and agencies[3] (hereafter referred to as the sponsor), the Council of Canadian Academies (CCA) convened an expert panel to review what is known about policies, strategies, and frameworks for identifying and protecting sensitive research of concern while balancing open science and innovation. Drawing on published evidence and interviews with policy-makers, practitioners, and academics, the panel explored measures to identify sensitive research, determine when it is of concern, and how to safeguard it throughout the three phases of the research process: the research design phase, the active research phase, and the post-research phase. The panel also considered enabling factors that support the implementation of these measures and open science. At the sponsor's request, the panel applied its findings to two areas—ocean research and pathogen research—to demonstrate how to protect research that could be weaponized and/or that has a strategic value for public health, safety, or security.

3 Fisheries and Oceans Canada; Environment and Climate Change Canada; National Research Council Canada; Natural Resources Canada; Transport Canada; Canadian Food Inspection Agency; Health Canada; Innovation, Science and Economic Development Canada; and Public Safety Canada.

## Answering the charge

**What policies, strategies, or frameworks could be applied to help researchers identify when their research is considered DURC?**[4]

To make an informed decision about the potential level of openness, those engaged in and overseeing research activities need to know how to identify sensitive research and determine when it becomes of concern because it presents additional risks that require mitigation. Lists are a common tool for helping researchers determine whether their research is sensitive and of concern. Various departments of the Government of Canada (e.g., Innovation, Science and Economic Development Canada, Global Affairs Canada) have adopted lists that have implications for research security, including goods and items subject to export controls, sanctioned persons and entities, and sensitive technologies and affiliations of concern. These lists can overlap and may also be combined to indicate that research is not only sensitive but becomes of concern (e.g., lists of sensitive research areas and affiliations of concern). In addition to lists, the research community in Canada and in other jurisdictions relies on risk assessments and consultations with external experts (e.g., Indigenous Peoples, defence or intelligence experts) to identify sensitive research of concern. Combined, lists, risk assessments, and external expertise provide an opportunity for a thorough identification of risks based on factors pertinent to the research project (e.g., sensitive research areas and affiliations of concern, geographic location of research activities, foreign partnerships).

**What principles or strategies could be applied to determine how to safeguard DURC?**

Once sensitive research has been identified and assessed to be of concern, various measures focusing on people, institutions, and research projects can

4 While the charge refers to *dual-use research of concern (DURC)*, this term is generally used to refer to life sciences research (Gov. of United States, 2024a). Throughout the report, the panel will use a broader term—*sensitive research of concern*—to include a variety of fields and disciplines that participate in the research enterprise.

safeguard it throughout its lifecycle and mitigate the identified risks. These measures include, but are not limited to, security screenings of researchers, due diligence of research proposals and partnerships, cybersecurity and physical security, and pre-publication reviews of research results. To be effective, measures to safeguard sensitive research of concern must be continuously reassessed throughout the research lifecycle, taking into account the research context and the need to support all phases of the research process. Most of these measures focus on the first two phases of the research process—research design and active research—to identify and mitigate risk as early as possible. Additional guidance focused on the post-research phase can enable responsible sharing of data and communication of research results, thereby advancing both open science and research security.

**What does current evidence suggest for identifying and protecting DURC while balancing open science and innovation?**

The panel found many promising measures to identify and safeguard sensitive research and sensitive research of concern. In recent years, Canada and its allies have increased focus on research security, which necessitates additional studies on the effectiveness of relevant measures. By enhancing our understanding of which measures are more effective, these studies can promote continuous learning and improvement, help balance research security and open science, optimize limited resources, and reduce the compliance burden placed on individual researchers and institutions.

### A modern research mindset is critical to building an open, innovative, and secure research system

Rapid technological advancement and shifting geopolitical contexts underscore the need for all actors in the research ecosystem to adopt a modern research mindset to navigate expectations around openness, collaboration, ethical conduct, and the safeguarding of sensitive information.

A **modern research mindset** is one where all actors participating in the research ecosystem are aware of the context in which they conduct research, its impacts on the world, and of the policies, principles, and practices to address these impacts, including research security, open science, Indigenous rights, data sovereignty, ethics, consent and research integrity. These policies, principles, and practices allow individuals to assess how open and secure their research needs to be.

A modern research mindset is a key competency in today's research landscape—one that embraces transparency and collaboration while also recognizing the critical importance of identifying and safeguarding sensitive research, adhering to security protocols, and mitigating risks such as foreign interference or data misuse. Cultivating this mindset is essential for successfully implementing research security measures in a way that also considers the imperatives of open science and innovation. It fosters a commitment to shared accountability, where responsibilities for research security are distributed across actors of the research ecosystem, including researchers, institutional leadership, research security staff, governments, and the private sector.

### Education, communication, and capacity-building can help cultivate the modern research mindset to enable researchers to successfully engage with both open science and research security

Education, communication, and capacity-building at individual and institutional levels can help cultivate a modern research mindset for individuals involved in the research ecosystem and foster widespread awareness and sensitivity to open science and research security issues. In Canada, entities such as Public Safety Canada's Research Security Centre, federal and provincial/territorial research funders, the Canadian Security Intelligence Service's Academic Outreach and Stakeholder Engagement program, and institutional research security units can provide guidance to the community. Research organizations across Canada have also come together to create national and regional communities of practice. These groups are critical in sharing advice and best practices across the research ecosystem. The Government of Canada has an opportunity to enhance these services through additional funding and improving communication channels among the intelligence community, researchers, and institutional administration.

Research security guidelines and frameworks in foreign jurisdictions (e.g., Australia, Germany, United Kingdom, United States) highlight the important

role of universities and university leadership in the provision of adequate support, training, and education to staff and students. For example, in Germany, some institutions have established specialized committees to help researchers identify sensitive research of concern. In the United States, the National Science Foundation supports the work of the SECURE Center—an information hub, which aims to facilitate collaboration on research security issues and provide guidance and information to the research community. Other research security measures include organization-wide awareness-building efforts, communication strategies, and regular general training on research security, research integrity, and conflicts of interest and commitment. General training can be customized to better address the needs of specific groups (e.g., researchers, students, administrative support services). Training focused on specific policy requirements can also enable compliance across research institutions in Canada.

### Harmonization of approaches to research security and open science can improve the effectiveness of relevant measures

Approaches to research security and open science differ across Canada, creating challenges for inter-institutional partnerships, the consistent implementation of research security measures, and research funding applicants and recipients supported by several funding agencies. This lack of harmonization places additional administrative burdens on researchers and weakens the uptake of initiatives. One way to address these issues is to establish common baseline criteria grounded in shared principles and approaches to key challenges, while allowing flexibility for tailored implementation to meet the specific needs of different contexts. This would help reduce duplication and administrative load for researchers and institutions working to deploy both research security and open science policies.

### Private sector participation in open science and research security practices is necessary to ensure the responsible sharing of research outcomes

The private sector makes important contributions to the Canadian research ecosystem, including in sensitive research areas such as quantum technologies, pathogens and toxins, and AI. Different orders of government exercise limited control over research security and open science practices when research is not publicly funded, which is a gap in the domestic approach to research security and open science alike. In recent years, the Government of Canada has intensified its security engagement with private companies in the biopharmaceutical, life sciences, and data science sectors, as well as with small- and medium-sized enterprises utilizing emerging technologies. A

similar trend can be observed in foreign jurisdictions. For example, in the United Kingdom, the National Protective Security Authority and the National Cyber Security Centre have created the Secure Innovation toolkit for private sector innovators, while the government's Engineering Biology Responsible Innovation Advisory Panel integrates industry into the governance of dual-use technologies. From 2020 to 2025, the U.S. National Academies of Sciences, Engineering, and Medicine conducted the Science, Technology, and Security Roundtable, where representatives from government, academia, and the private sector exchanged information and best practices related to research security. Developing similar inclusive approaches in Canada could facilitate information-sharing and reduce the exposure to threats across the entire research ecosystem.

### The success of measures that enable open science and research security initiatives requires sustained funding

Research security policies enacted by different orders of government increase the administrative burden on research organizations, highlighting the need for additional funding to support relevant programs and units in the private and public sectors. For example, additional resources are necessary when research security policies impose physical and cybersecurity requirements for storing, transmitting, and processing sensitive data and the safeguarding of equipment. The implementation of open science principles involves achieving FAIR (Findable, Accessible, Interoperable, and Reusable) data and adhering to TRUST (Transparency, Responsibility, User focus, Sustainability, and Technology) principles, all of which require extensive financial resources and infrastructure.

In Canada, federal research security funding is calculated as a percentage of each post-secondary institution's eligible direct research funding above $2 million, which creates differences in capacity between large universities and other institutions, including small- and medium-sized universities, healthcare institutions and affiliated research institutes, and colleges and polytechnics. Providing support for building research security and open science capacity across all post-secondary institutions could help address these disparities.

**How would the above approaches be applied in case studies related to research that could be weaponized or that has a strategic value for public health, safety, or security?**

At the sponsor's request, the panel applied its findings to two areas—ocean research and pathogen research—to demonstrate how to protect research that could be weaponized and/or that has a strategic value for public health, safety, or security.

### The security of ocean research can be enhanced with existing approaches that apply in other research areas and through Indigenous leadership

The risks associated with ocean research have received far less attention in policies and guidelines than other areas such as pathogen research, and there are no comprehensive measures to identify sensitive ocean research and determine when it is of concern. Safeguarding measures apply to ocean research on a case-by-case basis depending on the applicable policies of research institutions or funding requirements.

To enhance research security, ocean researchers need to be aware of and address a number of potential risk factors, most of which are not unique to ocean research. They include international partnerships, geography (e.g., research in the Arctic), the production and use of certain types of data and large datasets (e.g., personal data, spatial data), and research concerning certain technologies and research areas (e.g., some types of sonar, underwater wireless sensor networks). Research security policies promulgated by federal and provincial governments, as well as by some organizations conducting ocean research, can provide helpful guidance in the identification of risks.

Factors that indicate increased sensitivity can be grounds for directly applying safeguarding measures or conducting an additional risk assessment. Specialized committees can help researchers identify research as sensitive or sensitive of concern because it can be reasonably anticipated to be misappropriated or misused immediately or in the future, with little or no modification. Safeguarding measures that apply to other types of research (including pathogen research) can be extended to ocean research identified as sensitive or sensitive of concern.

While there are many promising approaches to ensuring the security of ocean research, their appropriateness for research involving First Nations, Inuit, and Métis can only be determined by the Indigenous communities themselves. In Canada, a rights-based framework for research involving Indigenous Peoples stems from the Constitution and the *United Nations Declaration on the Rights of Indigenous Peoples*, which stipulates that Indigenous Peoples have the right to self-determination in all aspects of research that affects them. Many Indigenous Peoples in Canada rely on marine ecosystems for subsistence and security. Indigenous leadership is instrumental in identifying and addressing

unique security and sovereignty challenges experienced by coastal communities due to climate change, coastal erosion, reduced access to marine resources, and increasing geopolitical tensions in the Arctic.

### Approaches to ensuring the security of pathogen research can be enhanced through self-enforcement of government research security policies and multidisciplinary risk assessments

Lists put forward by the Government of Canada are the main mechanism for identifying sensitive research involving certain types of human toxins and pathogens. Additional measures such as the review of research before publication and PHAC's risk assessment process supplement and reinforce the application of lists. The convergence of pathogen research and emerging technologies (e.g., nanotechnology, AI, quantum) challenges existing approaches to identifying sensitive research of concern. Laws, regulations, and policies that guide the identification of risks do not always keep pace with the rapid advancements in technology. These challenges can be addressed through a risk assessment process that draws on multidisciplinary expertise and considers additional risk factors.

In pathogen research, a host of measures to safeguard sensitive research of concern applies to the research design and active research phases of the research process. These measures include screening people working with security-sensitive biological agents, research licensing, controlled access to facilities, and additional cybersecurity requirements for some facilities. In addition to legal restrictions on research partnerships and collaborations, regulated facilities use internal policies and directives, non-disclosure agreements and training to safeguard their research, as well as limit the publication of outputs and data. The Policy on Sensitive Technology Research and Affiliations of Concern (STRAC) and the National Security Guidelines for Research Partnerships (NSGRP) are not always directly applicable to pathogen research; however, they can provide helpful guidance on how to avoid or mitigate security risks posed by certain collaborations and publications.

Similar to ocean research, the existing legal framework for pathogen research that involves Indigenous Peoples, their Land, and their data upholds Indigenous rights by affirming that such research should be co-led and co-developed with communities to comply with the principle of data sovereignty.

# Abbreviations

| | |
|---|---|
| CFI | Canada Foundation for Innovation |
| CIHR | Canadian Institutes of Health Research |
| CSIS | Canadian Security Intelligence Service |
| DMP | data management plan |
| DND | Department of National Defence |
| DRDC | Defence Research and Development Canada |
| DURC | dual-use research of concern |
| FAIR | Findable, Accessible, Interoperable and Reusable |
| FNIGC | First Nations Information Governance Centre |
| FRQ | Fonds de recherche du Québec |
| HPTA | *Human Pathogens and Toxins Act* |
| HPTR | *Human Pathogens and Toxins Regulations* |
| ISED | Innovation, Science and Economic Development Canada |
| KEF | Kommissionen für Ethik sicherheitsrelevanter Forschung (specialized research ethics committees for security-relevant research, Germany) |
| NASEM | National Academies of Sciences, Engineering, and Medicine (U.S.) |
| NRO | named research organization |
| NSGRP | National Security Guidelines for Research Partnerships |
| PHAC | Public Health Agency of Canada |
| RDM | research data management |
| SSBA | security sensitive biological agents |
| STRAC | Sensitive Technology Research and Affiliations of Concern |
| TCPS 2 | Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans |
| TRL | technology readiness level |
| TRUST | Transparency, Responsibility, User focus, Sustainability and Technology |
| UNDRIP | *United Nations Declaration on the Rights of Indigenous Peoples* |
| VIDO | Vaccine and Infectious Disease Organization |

# Contents

1

# Introduction

The concept of research security—that is, protecting research from misuse, theft, or other malicious activities—is not new. During World War II, scientists employed at the Los Alamos National Laboratory as part of the Manhattan Project to create the world's first atomic bomb became targets of espionage. Among other famous cases, the German theoretical physicist Klaus Fuchs served a nine-year prison sentence in the United Kingdom after the war, for stealing and supplying atomic secrets to the Soviet Union (Laucht, 2012). Research security developed as a subset of national security during the Cold War to protect the research enterprise from military technology espionage, often with a specific focus on research that could be considered dual use (i.e., have both military and civilian applications) (Wilner *et al*., 2022).

Today, the increased focus on research security is driven by the need to protect Canada's open, international, and collaborative R&D environment from state and non-state actors wishing to exploit it in order to gain an economic, political, or strategic advantage (SIGRE, 2022; ISED, 2023c). Canada's National Security and Intelligence Committee of Parliamentarians (NSICOP) has identified several risks driven by the geopolitical context, including espionage targeting domestic health, science, and technology sectors; cyber threats to critical infrastructure; potential use of nuclear, chemical, and biological weapons; and illicit and covert procurement of dual-use technologies (NSICOP, 2021). Based on documented incidents and publicly reported information, foreign interference in Canada has manifested through unauthorized research collaborations, the misuse of official positions for foreign interests, the covert transfer of sensitive technologies, and targeted cyber activities, posing significant threats to national security, intellectual property, and institutional integrity (CBC News, 2014, 2024; Cyber Centre, 2024a; RCMP, 2024).

The concept of *research security* includes policies and practices that protect sensitive research intended for beneficial purposes (ISED, 2023c) (e.g., pandemic preparedness, disaster resilience, navigation accuracy) from "risks of undue influence, interference, or misappropriation …; the outright theft of ideas, research outcomes, and intellectual property …; and other activities and behaviours that have adverse economic, strategic, and/or national security implications" (SIGRE, 2022).

As an element of national security, research security helps ensure that Canada's technological and industrial capabilities are protected from espionage, theft, and other external threats (NSERC, 2024a). As an element of economic security, it fosters innovation; helps prevent the loss of intellectual property, patent opportunities, and potential revenue; and protects organizational competitiveness (Asselin, 2024). Research security is important for all

researchers and organizations because it advances the responsible conduct of research, helps avoid reputational damage and legal liability, and fosters public trust (GC, 2022a; NSERC, 2024a; SIGRE, 2024). In the panel's opinion, all actors of the research ecosystem benefit from research security measures and share accountability for their implementation.

Research security is interconnected with other movements and practices that underpin the research enterprise, including open science. *Open science* aims "to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community" (UNESCO, 2021). By applying open science practices (e.g., participatory research; open software, hardware, data, access, and education resources), the research community can accelerate scientific discovery, facilitate evidence-based policy-making, make research more accessible to the general public, and increase public trust in the research enterprise (GC, 2020; UNESCO, 2021; COS, n.d.).

In the panel's opinion, in an era of increased emphasis on research security, the practice of open science helps mitigate the risk of oversecuritizing research, ensures the responsible sharing of research and data to advance knowledge and innovation, and supports everyone's right "to share in scientific advancement and its benefits" (UNGA, 1948). By enhancing accountability, transparency, and reproducibility in the research process and outcomes, open science promotes *responsible conduct of research*—that is, "the awareness and application of established professional norms, as well as values and ethical principles that are essential in the performance of all activities related to research" (GC, 2022b). Responsible conduct of research, in turn, supports open science by ensuring that research data, methods, and results are transparent, accurate, and handled in accordance with professional values, principles, and best practices that guide research communities.

In an era of increased emphasis on research security, the practice of open science helps mitigate the risk of oversecuritizing research

Although open science and research security can be perceived as opposing priorities because they focus on different goals, in practice, they are interconnected and work together to inform decisions about how, when, with whom, and to what extent research can be shared (NSERC, 2024a). These decisions are not always straightforward: they depend on both

objective and subjective factors (e.g., area of research, geopolitical developments, researchers' risk awareness, access to resources) and require an ongoing assessment of risks throughout the research lifecycle (Chapter 3). As a result of these assessments, some research may be subject to necessary restrictions on sharing, for example, because it poses risks to public health or national or economic security. In contrast, other types of research may be openly shared. In many instances, however, it is unclear which policies, strategies, or frameworks can identify the level of research openness and safeguard research identified as sensitive, and who bears the responsibility for implementing such frameworks effectively.

## 1.1 The charge to the panel

Recognizing the increased focus on and need for research security, as well as the value of open and collaborative research, Defence Research and Development Canada (DRDC) and the Public Health Agency of Canada (PHAC), with the support of other departments and agencies[1] (hereafter referred to as the sponsor), asked the Council of Canadian Academies (CCA) to answer the following question and sub-questions:

**What does current evidence suggest for identifying and protecting dual-use research of concern (DURC) while balancing open science and innovation?**[2]

- What policies, strategies, or frameworks could be applied to help researchers identify when their research is considered DURC?
- What principles or strategies could be applied to determine how to safeguard DURC?
- How would the above approaches be applied in case studies related to research that could be weaponized or that has a strategic value for public health, safety, or security?

The sponsor requested that, in answering the third sub-question of the charge, the panel focus on two areas—ocean research (including a wide range of fields

1 Fisheries and Oceans Canada; Environment and Climate Change Canada; National Research Council Canada; Natural Resources Canada; Transport Canada; Canadian Food Inspection Agency; Health Canada; Innovation, Science and Economic Development Canada; and Public Safety Canada.

2 While the charge refers to *dual-use research of concern (DURC)*, this term is generally associated with life sciences research (Gov. of United States, 2024a). Throughout the report, the panel will use a broader term—*sensitive research of concern*—to include a variety of fields and disciplines that participate in the research enterprise.

and types of research) and pathogen research[3]—and demonstrate the application of measures with the greatest potential to identify and safeguard sensitive research while balancing open science and innovation. The sponsor chose these areas to illustrate the application of the report's findings to research with different levels of regulatory oversight. To answer this aspect of the charge, the panel presents examples of measures and how they can be applied in these areas.

## 1.2 Terminology

During deliberations and evidence gathering, the panel encountered several terms and definitions that merit clarification (Box 1.1). While some of these definitions were taken directly from policies and literature, others were developed by the panel based on the analysis of policies adopted in Canada and select foreign jurisdictions (Aotearoa New Zealand, Australia, the EU, France, Germany, the Netherlands, the United Kingdom, the United States) (CCA, 2025).

### Box 1.1 Definitions of key terms

***Biosafety*** refers to "containment principles, technologies, and practices that are implemented to prevent unintentional exposure to regulated materials, and their accidental release" (PHAC, 2022).

***Biosecurity*** refers to "security measures designed to prevent the loss, theft, misuse, diversion, or intentional release of regulated materials, and other related assets (e.g., personnel, equipment, non-infectious material, animals, sensitive information)" (PHAC, 2022).

***Data sovereignty*** in the context of Indigenous rights can be defined as "Indigenous Peoples' right to maintain, control, protect and develop their cultural heritage, traditional knowledge and traditional cultural expressions, as well as their right to maintain, control, protect and develop their intellectual property over these" (Kukutai & Taylor, 2016).

***Dual-use research***, depending on the context, refers to scientific knowledge, technologies, data, and processes that: (i) have both potential civilian and military applications; or (ii) have the potential for both benevolent and malevolent applications (Kavouras & Charitidis, 2019) and the capacity to do harm on physiological, moral, or ethical

(continues)

3 The sponsor variably uses biosafety, biosecurity, and pathogen research to refer to this area of research. The term *pathogen research* is used throughout the report, as it reflects the focus of this research area.

(continued)

grounds (Evans & Commins, 2017). Almost all research can be dual use insofar as it can yield scientific knowledge, technologies, data, and processes with potential benevolent and malevolent applications (Kavouras & Charitidis, 2019; Lev, 2019; Kosal, 2020a).

***Dual-use research of concern (DURC)*** is adopted in the life sciences to refer to a subset of dual-use research that, "based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be misapplied to do harm with no, or only minor, modification to pose a significant threat with potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security" (Gov. of United States, 2024a).

***Indigenous research*** has been defined as "research in any field or discipline that is conducted by, grounded in or engaged with First Nations, Inuit, Métis or other Indigenous nations, communities, societies or individuals, and their wisdom, cultures, experiences or knowledge systems, as expressed in their dynamic forms, past and present. Indigenous research can embrace the intellectual, physical, emotional and/or spiritual dimensions of knowledge in creative and interconnected relationships with people, places and the natural environment" (Indigenous Advisory Circle & SSHRC, 2025).

A ***modern research mindset*** is one where all actors participating in the research ecosystem are aware of the context in which they conduct research, its impacts on the world, and of the policies, principles, and practices to address these impacts, including research security, open science, Indigenous rights, data sovereignty, ethics, consent, and research integrity. These policies, principles, and practices allow individuals to assess how open and secure their research needs to be.

***Open science*** is a combination of "movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community. It comprises all scientific disciplines and aspects of scholarly practices, including basic and applied sciences, natural and social sciences and the humanities, and it builds on the following key pillars: open scientific knowledge, open science infrastructures, science communication, open engagement of societal actors and open dialogue with other knowledge systems" (UNESCO, 2021).

(continues)

(continued)

***Research*** encompasses both the research process and outputs—including knowledge, goods, technologies, and data—in various fields. It includes both fundamental and applied research, as well as publicly and non-publicly funded research activities.

***Research security*** encompasses a suite of actions and activities intended to identify and protect sensitive research from risks, including, but not limited to, "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 activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications" (SIGRE, 2022).

***Responsible conduct of research*** is "the behaviour expected of anyone who conducts or supports research activities throughout the life cycle of a research project (i.e., from the formulation of the research question, through the design, conduct, collection of data, and analysis of the research, to its reporting, publication and dissemination, as well as the management of research funds). It involves the awareness and application of established professional norms, as well as values and ethical principles that are essential in the performance of all activities related to research. These values include honesty, fairness, trust, accountability, and openness" (GC, 2022b).

***Sensitive research*** refers to the research process and outputs—including but not limited to knowledge, goods, technologies, and data—in a variety of fields that, while intended for beneficial purposes, may be used by nefarious actors or for nefarious purposes to harm the public, public health and safety, the environment, agriculture, fisheries, sovereignty, and economic and national security in Canada and internationally, or pose privacy and ethics risks (Gov. of New Zealand, 2022; Leopoldina & DFG, 2022a; ISED, 2023a,b; JASON, 2024). The panel acknowledges that this list of potential harms and risks is non-exhaustive and may change depending on the evolving geopolitical context.

***Sensitive research of concern*** is a subset of sensitive research that can reasonably be anticipated to be misappropriated or misused immediately or in the future, with minimal or no modifications, and that needs to be subject to additional safeguards (Leopoldina & DFG, 2022a; ISED, 2023a,b; JASON, 2024).

To provide researchers with clear guidance, the panel focused this assessment on measures to identify and safeguard sensitive research of concern, as this research, if misused or misappropriated, presents the greatest risks. While the sponsor's charge focuses on *dual-use research of concern*, this term is predominantly associated with the life sciences (Gov. of United States, 2024a). The sponsor asked the panel to address research security concerns arising in various fields and disciplines and gave it discretion to make terminology choices that would allow it to fully answer the charge. Thus, throughout the report, the panel will use a broader term, *sensitive research of concern*, instead of DURC, to reflect the fact that the scope of the assessment extends to research security issues arising across and in a variety of fields, including social sciences and humanities. The panel also notes that this terminology is aligned with the approach taken by the Government of Canada, which calls on researchers to assess the sensitivity of research projects (ISED, 2024a; NSERC, 2024b). The panel acknowledges that in the context of pathogen research, the term DURC remains widely used in policies and guidelines (e.g., PHAC, 2018a; NSABB, 2023). Terminology differences will be noted with a footnote when cited references use an alternate term.

## 1.3 Sensitive research and Indigenous rights

In Canada, Indigenous Peoples are involved in research in various ways—as researchers, communities, and research participants and subjects. Information collected by, for, and about Indigenous people and communities in any research context, including pathogen and ocean research, can be sensitive and require safeguarding for such reasons as privacy, community and cultural significance, and the risk of misuse and exploitation (UN, 2007; de Beer & Dylan, 2015; CCA, 2023a). "Open science and research security can encompass many interconnected considerations, including the ability of communities to safely live their lives, have access to food and housing, ensure the physical safety of researchers and protect the Land, individual and collective privacy rights, and health data from exploitation" (N. Weetaluktuk, personal communication, 2025).

### 1.3.1 A rights-based framework

Standards for equitable research involving Indigenous Peoples and their Lands are set out in the *United Nations Declaration on the Rights of Indigenous Peoples* (UNDRIP) (UN, 2007). UNDRIP was codified into federal law in Canada in 2021 and provides a legal foundation for governmental and institutional relationships with Indigenous Peoples (JUS, 2021). Several UNDRIP provisions

(Articles 3, 11.1, 13.1, 14.1, 18, 19, 26, 27, 28, 29.1, 31, 32) support the rights of Indigenous Peoples to self-determination with respect to research activities that affect them, as well as their data, knowledge, and Lands (UN, 2007). The provisions of UNDRIP must be considered when developing research security and open science policies.

In Canada, the land on which research takes place may be subject to constitutionally protected Indigenous and treaty rights (GC, 1982). This rights-based framework has specific applications in both research areas explored in the report. In ocean research, where there is a particular focus on the Arctic, much of this area is subject to land claim agreements, which set out Indigenous rights and governance of the Land (ITK, 2018; CIRNAC, 2022a). Therefore, the identification and safeguarding of sensitive research of concern in these areas, as well as any other coastal and ocean areas involving Indigenous Peoples or Lands, require that research projects and protocols be co-developed and co-led by Indigenous communities to reflect unique research contexts and ensure cultural safety and mutually beneficial research outcomes. Community leadership and engagement are instrumental to understanding distinct security and sovereignty challenges experienced by Indigenous coastal communities, which can include those due to climate change, coastal erosion, and reduced access to marine resources (Leonard *et al.*, 2022; Whalen *et al.*, 2022). These challenges are exacerbated in the Arctic, which presents particular interest to the sponsor due to increasing geopolitical tensions (Box 1.3).

Similar to ocean research, Canada's legal framework upholds a rights-based approach to conducting pathogen research that involves Indigenous Peoples, their Land, and their data, and highlights that such research should be co-led and co-developed with communities to comply with the principle of data sovereignty (UN, 2007).

> The principle of data sovereignty and the inherent right of Indigenous Peoples to control how their data are accessed and used are instrumental in the design and implementation of any research security and open science policies

### 1.3.2 Data sovereignty

The concept of data sovereignty refers to "meaningful control, ownership, and other claims to data articulated by a variety of agents ranging from individuals to countries" (Hummel *et al.*, 2021). Interpretations and applications of the principle of data sovereignty are influenced by the geopolitical context and national priorities, which may change over time (Hummel *et al.*, 2021; Belli *et al.*, 2024; GC, 2025a). In the context of Indigenous rights, data sovereignty can be defined as

"Indigenous Peoples' right to maintain, control, protect and develop their cultural heritage, traditional knowledge and traditional cultural expressions, as well as their right to maintain, control, protect and develop their intellectual property over these" (Kukutai & Taylor, 2016) (Box 1.2). The principle of data sovereignty applies to all entities conducting Indigenous research, including government departments and agencies that have a constitutional duty to consult Indigenous Peoples and provide appropriate accommodation when planning activities that may impact their rights (UN, 2007; GC, 2025b). In the panel's opinion, the principle of data sovereignty and the inherent right of Indigenous Peoples to control how their data are accessed and used are instrumental in the design and implementation of any research security and open science policies. The right of Indigenous Peoples to be involved in the co-development of research on their Lands includes an examination of what research security is, how research is controlled, and from whom research needs to be protected.

## Box 1.2 Initiatives advancing data sovereignty in Canada

For First Nations in Canada, the First Nations Information Governance Centre (FNIGC) administers the principles of ownership, control, access, and possession of data (commonly referred to as OCAP®[4]), which assert "that First Nations alone have control over data collection processes in their communities, and that they own and control how this information can be stored, interpreted, used, or shared" (FNIGC, n.d.). OCAP®, thus, is explicitly tied to considerations of open science and research security; the responsibility and right to determine the sensitivity of First Nations information lie with the First Nations individuals or communities implicated in the research. Researchers should not see OCAP® as a hindrance or an obstacle to their research activities, but as a stepping stone to relationship-building and advancing First Nations' perspectives on open science and research security (Konczi & Bill, 2024).

Budget 2021 allocated funding to advance data sovereignty for Inuit and Métis individuals and communities, supporting "baseline data capacity and the development of distinctions-based Inuit and Métis Nation data strategies" (GC, 2021a). In 2022, Inuit Tapiriit Kanatami committed $4 million for the creation of an Inuit data strategy to support regionally

(continues)

4 OCAP® is a registered trademark of FNIGC. To better understand these principles, see their website at https://fnigc.ca/ocap-training/.

(continued)

specific strategies across Inuit Nunangat (ITK, 2018; Jamal, 2022). In the panel's opinion, any research involving Indigenous Peoples or their Lands should be treated as sensitive by default because it implicates Indigenous rights (which can cross state borders) and requires consent of the communities in question (CIHR *et al.*, 2022).

## 1.4 The panel's approach

To answer the charge, the CCA convened a multidisciplinary and multisectoral panel of 13 experts (hereafter referred to as the panel). Panel members were selected for their expertise in national and research security, the post-secondary research ecosystem, research infrastructure, nuclear policy, epidemiology and pathogen research, ocean research, contributions to open science, biosafety, and bioethics, as well as experience in implementing research security policies. Panel members served pro bono and were tasked with conducting a thorough and objective assessment of the available evidence. The panel met five times virtually and two times in person over a period of 11 months, between July 2024 and June 2025, to develop this report.

To ensure the integrity of the assessment process, panel members were required to disclose to the CCA and fellow panellists any conflicts of interest—actual, foreseeable, or perceived—relevant to the issues being discussed so these could be managed transparently. Panel members abided by a confidentiality agreement and code of conduct designed to support an environment that fosters collaborative and respectful deliberations, the free exchange of knowledge, and the synthesis of evidence. To maintain the panel's independence, the sponsor did not appoint panel members, nor did it engage with the panel during the assessment process, with the following exceptions: (i) at the panel's first meeting, where the sponsor was invited to present the charge, and (ii) at a briefing scheduled after the panel had formally signed off on the report prior to its public release, where the panel presented the main findings to the sponsor.

The report underwent a comprehensive peer review, whereby an additional 13 experts from Canada and abroad provided further evidence, expertise, and knowledge. Like panel members, peer reviewers participated as individuals and not as representatives of their respective organizations. Peer reviewers provided feedback to inform panel deliberations but were not asked to endorse the final report. They remained anonymous until the report was released. This

process was overseen by an independent peer review monitor appointed from the CCA's Scientific Advisory Committee, further supporting the integrity of the review.

### 1.4.1 Evidence and scope

The panel's assessment was based on a review and synthesis of diverse sources of evidence, including peer-reviewed publications and grey literature (i.e., policy documents, government publications, websites, and reports by national and international organizations and committees). The panel conducted keyword-based searches of published literature using several databases and explored the websites of relevant government departments and agencies in Canada and select foreign jurisdictions (Aotearoa New Zealand, Australia, the EU, France, Germany, the Netherlands, the United Kingdom, the United States), examining relevant legislation, policies, and guidelines relating to research security measures to form an evidence base to answer the charge (CCA, 2025). This report is not based on a systematic review, but rather on a detailed synthesis of key references, informed by a jurisdictional scan and as identified by the panel ((CCA, 2025); available on the CCA website).

The panel collected additional evidence through semi-structured interviews to better understand the breadth of perspectives on sensitive research and related areas. The panel interviewed Indigenous researchers and those engaged with Indigenous organizations working with data sovereignty, open science, and research security to ensure that these perspectives were considered alongside measures to identify and safeguard sensitive research of concern. In addition, the panel interviewed practitioners and academics in the two research areas of interest to the sponsor.

The review of evidence did not focus on issues related to misinformation, disinformation, and alteration of data and knowledge by malicious actors, or comprehensive program and policy evaluations, as these areas were considered out of scope.

The panel collected evidence between July 2024 and June 2025. The panel notes that the rapidly changing geopolitical context may result in some of the measures identified in this report being altered or withdrawn in the near future.

### 1.4.2 Research areas

The panel was charged with demonstrating how research security measures explored in the report could be employed in two areas: ocean research and pathogen research. These two areas have markedly different levels of oversight and awareness of research security concerns and approaches.

#### The identification and safeguarding of sensitive research of concern is formalized in pathogen research, but existing frameworks cannot fully address the complexity of the research enterprise

Pathogen research is crucial to both society and the economy in Canada. It is a key driver of improved healthcare, increasing quality of life and longevity (Uhlenhaut *et al.*, 2013), and has also had enormous benefits for humanity through advances in biotechnology, including in food production, (bio)medicine, synthesis of biopharmaceuticals, (bio)materials, environment, energy, and counter-bioterrorism measures (Rappert & Selgelid, 2013; Rohden & Wieden, 2022). Further, the growing use of life sciences methods in industrial processes is laying the groundwork for a rapidly developing bioeconomy (Rohden & Wieden, 2022). Biotechnology is also expected to drive industry research, education, and employment in the life sciences, supporting further innovation and discovery (RBC Thought Leadership, 2024).

Pathogen research categorized as sensitive research of concern[5] can be critical to public health, pandemic preparedness, and agriculture, and its findings inform broader scientific advancements (NIH, 2014; Wang *et al.*, 2025). Given these benefits, concluding that a research project is of concern and that research can be used to cause harm does not mean it should not be funded, conducted, or shared. Instead, it means that researchers and institutions need to minimize the possibility of misuse by developing and implementing appropriate safeguarding measures (NIH, 2014). Arguably, the potential harm could be on a scale comparable to the good that positive applications can achieve.

The identification and safeguarding of sensitive research of concern involving pathogens are formalized through international instruments (e.g., WHO, 2022) and domestic laws, regulations, and guidelines (Chapters 3 and 4). According to the 2021 Global Health Security Index, Canada ranks first globally in terms of biosafety and third in terms of biosecurity (GHS Index, 2021; HC & PHAC, 2022). However, even when risk identification and assessment are formalized, existing frameworks cannot fully address the complexity of the research enterprise; circumstances can arise throughout the research process that lead to additional

5 NIH (2014) uses the term DURC.

risks. In Canada, existing measures to safeguard sensitive research of concern focus on biosafety and biosecurity, while rules regarding cybersecurity, research collaborations, and the responsible sharing and communication of research data are less clear (Chapter 4).

### There is a lack of guidance on identifying and safeguarding sensitive ocean research

Ocean research, especially work using observational and predictive sciences, is increasingly open and available to the public and international bodies in the interests of climate modelling and safer marine traversal (e.g., CIOOS, n.d.-a,-b; ONC, n.d.-a). Open-access data identifying the location of various resources (e.g., fish shoals, mineral deposits) could have enormous value for both resource management and exploitation (Loft & Saumweber, 2020). Ocean floor mapping and depth of water (i.e., bathymetric) data aid in sustainable ocean management, geohazard identification, and understanding climate change (Wölfl *et al.*, 2019). Up-to-date and accurate forecasting is crucial for maintaining industry and economic operations, environmental security, and human safety (GC, 2025c). In addition, monitoring ocean conditions is critical for climate modelling and requires regional and international cooperation to acquire accurate global information (e.g., Fujii *et al.*, 2019; Révelard *et al.*, 2022). Ocean data is collected by many actors, including researchers, the government (e.g., the Department of National Defence, Transport Canada, the Canadian Coast Guard), private companies, and non-governmental organizations (Iverson *et al.*, 2019; CIRNAC, 2022b; Moran *et al.*, 2022; DRDC, 2023; POLAR, 2023; GC, 2025d; GFW, n.d.).

Canada participates in international ocean predictive services and observational networks, all of which rely on a certain level of openness and accessibility of Canadian ocean data (e.g., Global Ocean Observing System, International Hydrographic Organization) (IHO, 2021; DFO, 2022; CIOOS, n.d.-a). Many research outcomes (e.g., ocean observation, monitoring, tracking) are expected to be made open and accessible to mitigate the effects of climate change and ensure navigation safety. However, these data could also be used for covert navigation and evading surveillance within Canadian waters.

Open access to real-time data regarding sea ice and weather forecasting is a critical need in the Arctic Ocean (Smith *et al.*, 2019). The region experiences many of the leading effects of climate change (e.g., Rantanen *et al.*, 2022); the ecological and social costs of these impacts, and the related physical data describing its changing environment, are valuable for modelling future climate scenarios and mitigation strategies at various scales (IPCC, 2019; Gaffey *et al.*, 2024). Such disruptions also significantly threaten the health and well-being of

Indigenous Peoples living in Arctic areas, who face disproportionate and interrelated impacts of climate change on food security and cultural identity (POLAR, 2022). Taken together, these factors underscore the importance of Arctic Ocean climate research, including research with Indigenous leadership or co-management (POLAR, 2022).

The sponsor requested that, in the context of examining ocean research as a focal area, the panel pay particular attention to research security in the Arctic Ocean. The panel notes that: (i) it is the region where divergent interests are colliding, to the detriment of effective scientific collaboration, and (ii) the level of research openness can be informed by changing national priorities and geopolitical context (Box 1.3).

## Box 1.3 Research security in the Arctic

Many jurisdictions have defined scientific research as a key element of their Arctic policies (Heininen *et al.*, 2020). China has been focusing on expanding scientific collaborations with Arctic states in the areas of remote sensing, space observations, and climate change research, prompting concerns about potential military applications of these research activities (Robinson, 2020; Falco *et al.*, 2024; Weisko, 2025). Moreover, in recent years, China and Russia have been ramping up their collaborations in the Arctic, with Russia increasingly reliant on China to fund and support the development of research and infrastructure projects due to sanctions imposed by other countries following the invasion of Ukraine (Funaiole *et al.*, 2023; GC, 2024a). These trends increase China's presence in the Arctic, which can pose significant threats to Canada's national security (GC, 2024a). The increased navigability of the maritime Arctic due to climate change also raises national security considerations, including asserting sovereignty in the area and bolstering security capacity (SECD, 2023).

The difficulty of providing clear guidance on identifying and safeguarding sensitive ocean research is exacerbated by the fact that ocean sciences are broad and encompass "all research disciplines related to the study of the ocean, the coast, and their relationships with societies: the natural, health, and social sciences, as well as engineering, the humanities, and multidisciplinary research" (CCA, 2013). According to the Woods Hole Oceanographic Institution, ocean research includes the study of climate and weather, coastal science, hazards, ocean chemistry, ocean circulation, ocean life, ocean resources and

policy, polar systems, pollution, seafloor, ocean technology, and underwater archaeology (WHOI, n.d.). Within each of these areas, there are further research specializations. For example, ship tracking is an important field of research in ocean technology because it helps ensure maritime safety and informs environmental decision-making (Nicoll *et al.*, 2025). Beyond the breadth and diversity of disciplines involved, ocean research may also be interdisciplinary or transdisciplinary.

## 1.5 Report structure

This report describes measures (i.e., policies, strategies, or frameworks) that could help the research community identify and safeguard sensitive research of concern while balancing open science and innovation. It then applies these measures to ocean and pathogen research. **Chapter 2** provides the context for the rest of the report by focusing on the research landscape in Canada through the lens of security and open science. **Chapters 3 and 4** describe measures that can help the research community identify and safeguard sensitive research of concern throughout the research process—the research design phase, the active research phase, and the post-research phase. These measures are then applied to ocean and pathogen research through current and hypothetical examples. **Chapter 5** describes the enabling factors that can help facilitate the measures outlined in the preceding two chapters. **Chapter 6** summarizes the application of measures to ocean and pathogen research, concluding with the panel's high-level reflections. It emphasizes that measures must be adopted holistically across all phases of the research process and supported by a system of shared accountability to be most effective.

2

# The Research Landscape in Canada

## Chapter findings

- Canada's decentralized and internationalized research ecosystem presents opportunities for conducting world-class research in sensitive technology areas that offer significant benefits for scientific development and society more broadly.
- There is limited state oversight of non-government-funded sensitive research in the current approach to research security and open science in Canada.
- The private sector is an important actor in Canada's research ecosystem, and its participation in open science and research security measures is necessary to ensure the responsible sharing of all research outcomes.
- The funding of research by foreign multinational entities is outside the scope of Canadian federal jurisdiction, which is a gap in the domestic approach to research security.
- Government efforts to promote the uptake of open science in Canada have focused on open-access publications. Measures that support responsible management and sharing of research data are new and require resources, training, and incentives to be successfully implemented across the research ecosystem.

Canada's research ecosystem has produced world-class research, including in sensitive technology areas, delivering benefits to science and society. However, as the research ecosystem becomes more internationalized and decentralized (Section 2.1), governments and institutions can lose control over how research, including sensitive research, is conducted, safeguarded, and shared (Section 2.2). Governments have implemented open science and research security policies to address this problem, but these policies need to be better applied and interconnected to fully realize the principle that "research should be as open as possible and as secure as necessary" (ISED, 2023a) (Sections 2.3 and 2.4).

## 2.1 Research ecosystem actors

The *higher education sector*, which includes universities, colleges, polytechnics, healthcare institutions and affiliated research institutes, generates much of the fundamental research and many of the technological applications that are eventually commercialized. Canada's R&D expenditures in the higher education

sector—over $18 billion in 2024 (StatCan, 2024a)—are proportionally higher than in most peer countries.[6] In 2022, Canada had the second-highest higher education R&D intensity (spending as a percentage of GDP) across G7 countries (OECD, 2025). The Government of Canada has directed significant investments toward maintaining and building on areas of post-secondary research where Canada holds leading positions, many of which overlap with potentially sensitive areas of research. For example, in quantum technology, Canada is a leader in domestic R&D at public institutions, and the federal government has recently launched a national quantum strategy (ISED, 2022a; CCA, 2023b). AI is another area where the federal government has invested over $2 billion since 2017 (PMO, 2024a) and pledged over $2 billion more in Budget 2024 (GC, 2024b).

Post-secondary institutions in Canada are also training graduate students at a growing pace: more than twice as many PhDs were conferred in 2022 than in 2002 (StatCan, 2024b). Canada's graduate student body is highly international, particularly in technologically intensive fields; however, federal caps on international students introduced in 2024 and 2025, as well as research security policies, may affect this trend (GC, 2025e) (Section 2.4). More than 50% of the PhDs conferred in 2021 in STEM and health fields[7] were granted to international students (StatCan, 2023), who may choose to leave Canada following the completion of their studies (CCA, 2021), contributing to the loss of opportunities for Canadian research and innovation. Factors such as language skills, expensive and lengthy immigration processes, time spent in the country of study, as well as socioeconomic and political conditions (in both country of study and home country) inform the retention of international PhD graduates (Trevena, 2019; Grewal, 2022; Malik *et al.*, 2022; Richardson & Hussain, 2022).

The *private sector* (e.g., industry, startups, foreign multinational companies) also conducts fundamental and applied research, but, in 2022, Canada's business enterprise R&D intensity was the second-lowest in the G7 (OECD, 2025). Despite a relatively low level of research activity, some private research could be considered sensitive, necessitating careful oversight and risk assessment. For instance, pharmaceutical companies engaged in developing new vaccine platforms, such as mRNA vaccines, are working on technologies that prevent infectious diseases but can also be used for pathogen engineering, which could be detrimental to human health if used for nefarious purposes (Musunuri *et al.*, 2021; Sandbrink & Koblentz, 2022). As of 2019, it is estimated that 70% of

6 According to StatCan (2020) "the higher education sector is composed of all universities, colleges of technology and other institute[s] of post-secondary education, whatever their source of finance or legal status. It also includes all research institutes, experimental stations and clinics operating under the direct control of, or administered by, or associated with, the higher education establishments."

7 According to the Statistics Canada categories of "physical and life sciences and technologies," "mathematics, computer and information sciences," and "health and related fields" (StatCan, 2023).

Pathogen and Toxin Licences issued by PHAC were granted to the private sector (PHAC, 2020; Gryphon Scientific, LLC, 2023). The panel notes, however, that the number of issued licences may not reflect the private sector's share of pathogen research activities.

Various *orders of government* participate in the research ecosystem as researchers, research funders, and regulators. The federal government sets international trade policy (including export controls on goods and technology) by creating policy frameworks relating to national defence, competition, and IP (GC, 1982, 1985a, 2025f; de Beer, n.d.); conducts R&D and talent development to support the private sector and the delivery of public mandates (ISED, 2025); and provides national-scale research infrastructure, including 19 research facilities funded by the Canada Foundation for Innovation (CFI) (CFI, n.d.-a). PHAC is responsible for the administration and enforcement of laws and regulations that "promote and protect the health, safety and security of Canadians" and minimize the risks of research involving pathogens and toxins (PHAC, 2022, 2024a).

Provincial and territorial governments have roles in education, intramural research, research funding and licensing, the provision of science infrastructure and health services, and support for regional centres of expertise (CCA, 2017, 2023a). Provincial and territorial jurisdiction over post-secondary education complicates the harmonization of research security policies across the country (Section 5.1).

As rights-holders, *First Nations, Inuit, and Métis* are entitled to determine what research activities can occur on their Lands, to control data related to their territories, Lands, knowledge, and language, and to determine what happens with the data and knowledge gained through those research activities (UN, 2007). Indigenous Peoples also actively participate in research activities as knowledge-holders, researchers, and research subjects (GC, 2019a).

## 2.2 Features of the research ecosystem

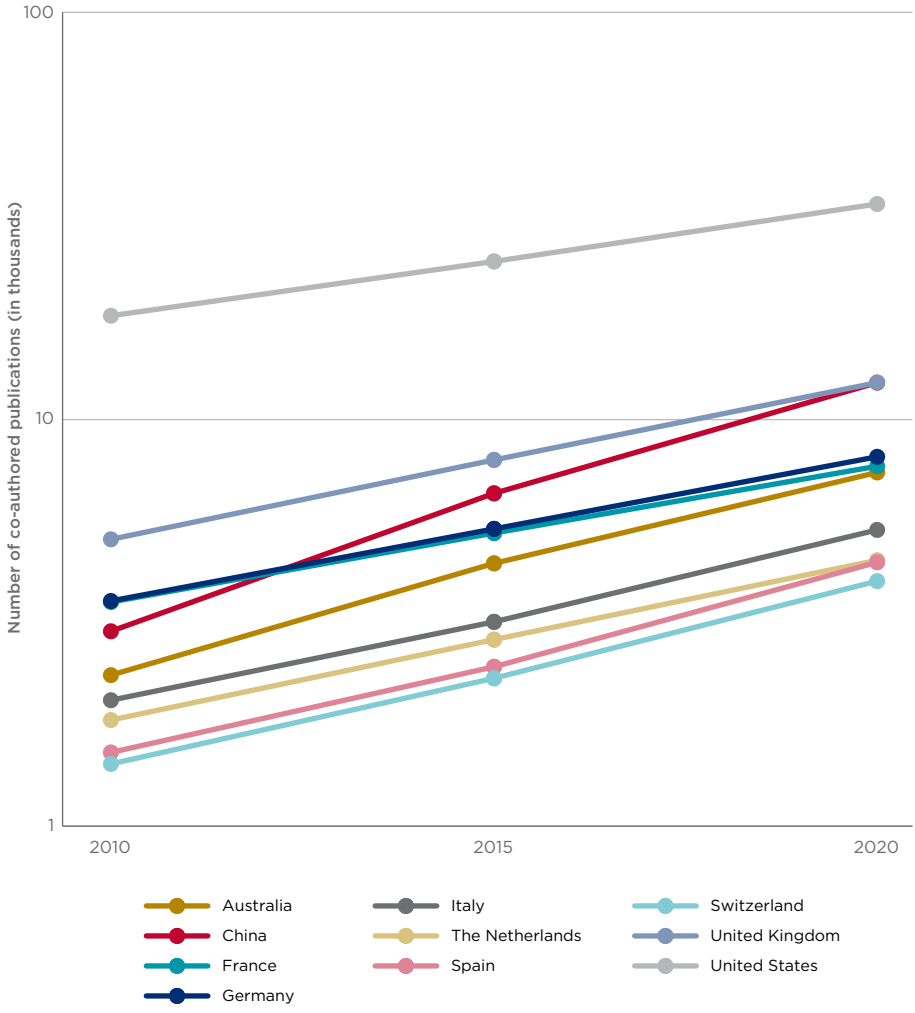
### Canada's research ecosystem benefits from international and intersectoral collaborations

Interdisciplinary and intersectoral collaborations are an important feature of the Canadian research landscape. Canada has one of the highest rates of business investment in R&D performed by the higher education sector among members of the OECD, accounting for ~7–8% of funding between 2010 and 2022 (OECD, 2025). Canada's research in highly competitive fields such as AI involves investments from the public, philanthropic, and private sectors (notably by

foreign multinational companies) (Brandusescu, 2021; U of T, 2022; Geremia, 2024).

Collaborations across disciplines or economic sectors are supported through granting programs (e.g., Alliance grants, New Frontiers in Research Fund, Canada First Research Excellence Fund) to encourage technological breakthroughs and high-risk, high-reward research with international and domestic private sector partners (GC, 2022c; NSERC, 2024c; CRCC, 2025). The Department of National Defence (DND) has been collaborating with the private and academic sectors to harness the benefits of innovation. In 2018, DND launched the Innovation for Defence Excellence and Security (IDEaS) program to enhance national defence and security capacity through demand-driven challenges for Canadian innovators (DND, 2023). As of March 2023, IDEaS has launched 75 challenges and invested over $330 million in projects. The majority of funding has been allocated to small- and medium-sized enterprises (53%), academia (27%), and large industry (17%) (DND, 2024a). Researchers within government science-based departments and agencies can collaborate internationally, including with private sector partners. For example, between 2012 and 2023, scientists at Fisheries and Oceans Canada co-authored 6,623 academic papers, 54% of which involved international collaborators and 11% included authors affiliated with for-profit organizations (Science-Metrix, 2024).

Canadian researchers are also active in international collaborations. Based on the number of co-authored publications in the Web of Science, the United States is Canada's most frequent collaborator, with 33,841 articles published in 2020 (Figure 2.1). The United Kingdom and China are second and third, respectively. Between 2010 and 2020, collaborations between researchers in Canada and China increased by more than 75% (CCA, 2024a), which represents a shift from less frequent bilateral collaborations in the early 2000s. The panel notes that these publications reflect research collaboration that happened before the introduction of federal and provincial research security policies (Section 2.4). It is unclear if this upward trend will hold due to the cooling of the Canada–China relationship in recent years. The federal government relies on official science and technology agreements and partnerships with other jurisdictions to cement Canada's place in the global research community (e.g., PMO, 2024b; GC, 1986). For example, in 2024, Canada and the EU signed an agreement that allows Canadian researchers and organizations to participate in Pillar II of Horizon Europe on the same conditions as their EU peers (EC, n.d.-a).




Source: CCA (2024a)

## Figure 2.1 Canada's top ten collaborating countries by co-authorship

Canada's top collaborating countries based on the number of co-authored publications in Web of Science between 2010 and 2020.

Partnerships and collaborative research are often seen as catalysts for discovery and hailed for leveraging complementary skills and resources (TRIUMF, 2018; CCA, 2024a). However, Canada's decentralized research ecosystem is also

vulnerable to security risks posed by the growing number of participants possessing distinct motivations, values, and incentives. Due to a lack of centralized oversight, threats to data, information, knowledge, and IP can arise from attacks by malicious actors or accidental disclosure (Wilner *et al.*, 2022). In research areas where Canada possesses strengths, the stakes are higher because these areas are more likely to attract malicious actors seeking to misuse or misappropriate data, knowledge, technology, or IP (e.g., Cyber Centre, 2024a). A lack of awareness of threats among researchers or the rejection of standard security procedures and protocols can exacerbate these vulnerabilities (Cyber Centre, 2024b; ISED, 2024b).

### Sensitive research activities are taking place in locations that are increasingly open and outside the jurisdiction of existing government oversight

The history of sensitive research is marked by several examples of technologies ubiquitous in civilian life after being discovered or first researched in government-funded military or industrial R&D settings. Although the internet, global-positioning systems, and AI models are shaped by decades of development work across several sectors, all three originated in research activities either carried out or funded by the U.S. government (Evan & Hays, 2006; Mowery, 2010; Lukasik, 2011; Ueno, 2023). Similarly, U.S. military procurement programs supported private laboratories, such as Bell Labs, working on electronics and semiconductors (Holbrook, 1995; Nokia Bell Labs, 2022). Technologies and processes developed or funded by the U.S. government still feature prominently on export control lists (GC, 2025f).

In the past several decades, sensitive technologies have also been developed independently of government-funded R&D. For example, quantum technologies, CRISPR-Cas9, and recent implementations of AI involve early-stage R&D borne out of basic research in the academic sector and increasingly funded by the private sector (Zhang, 2019; Pannier, 2023; Major *et al.*, 2024). The development of technologies with dual-use potential outside of direct state jurisdiction reduces governmental control over research activities and the sharing of research results. In consulting with foreign policy officials from the European Commission, France, and the United States, Pannier (2023) found that governments were made uneasy by the significant role played by large multinational enterprises (MNEs), since their decisions surrounding the location of R&D activities and the choice of partnerships do not take into account existing bilateral alliances between states and a state's sovereignty or national security priorities. These challenges can be exacerbated by the fact that some profit-seeking entities may be wholly or partially state-owned and aligned with foreign government interests (Jin *et al.*, 2022; Libman *et al.*, 2022).

The participation of some foreign private companies in sensitive research further highlights the vulnerabilities surrounding the loss of research, data, knowledge, information, and IP due to malicious actions or inadvertent disclosure (Wilner *et al.*, 2022; CSIS, 2024a).

In Canada, MNEs were responsible for the vast majority (76%) of business R&D expenditures in 2022, with foreign MNEs accounting for the largest share (44%), followed by Canadian MNEs (32%) and non-multinationals (24%) (StatCan, 2024c). The funding of research by foreign MNEs is currently outside the scope of Canadian federal jurisdiction. In the panel's view, this represents a gap in the domestic approach to research security, which focuses on protecting only some publicly funded research. The Business Council of Canada, representing over 170 Canadian companies, has suggested that, to ensure economic security, the federal government focus its efforts on supporting collaborations among Canadian private, public, and academic sectors and on adopting policies to replace problematic foreign sources of financing for academic research (BCC, 2023, n.d.). A number of enabling factors can bolster domestic research security across all sectors while harnessing the potential of non-government-funded research and innovation (Chapter 5).

### Arctic research remains a priority for Canada, but comes with geopolitical security challenges

Several foreign jurisdictions have increased their presence in the Arctic through strategic policies targeting research, security, or other factors (Heininen *et al.*, 2020; POLAR, 2020; IARPC, 2021; Gov. of United States, 2022a; Eiterjord, 2023; Lipunov & Devyatkin, 2023). These policies are driven by interests and values that are not always aligned with those of Canada and may be fraught with geopolitical tensions. Adversarial relations among China, Russia, and the United States are playing out in the Arctic for strategic reasons and due to gaps in Arctic governance (Zandee *et al.*, 2020; Cunningham, 2024; Tatlow, 2024). Although Canada relies on international research collaborations to enhance knowledge of the Arctic region, including about biodiversity and climate change, efforts to establish research partnerships may be hampered by geopolitical developments (GC, 2024a). For example, the interruption of collaborations with Russia following its invasion of Ukraine has prompted the former to cease providing its share of Arctic climate data—describing nearly half of the region—to the detriment of widely used climate modelling efforts (Breum, 2024).

The research efforts of other countries in the Arctic present concerns for Canada's national security (Tatlow, 2024) because physical geoscientific data collected in the course of research activities can be used to assert presence or

dominance in northern geopolitically contested areas (Eiterjord, 2024). The expansion of unmanned sensing infrastructure and the establishment of satellite ground stations—ostensibly used for scientific purposes (e.g., to facilitate data transfer from sensing infrastructure)—is one example of sensitive research activities in the Arctic, as collected data can be used for military surveillance purposes (Thomson, 2017; Falco *et al.*, 2024). Another example is underwater sensing technologies that can be used by foreign actors to examine the ocean floor for mineral resources located in the Arctic Ocean (Sun *et al.*, 2021; DND, 2024b). It has been argued that China pursues research efforts in the Arctic to solidify its position in the region, secure trade routes through the Northwest Passage, and explore resources (e.g., Brady, 2017; Eiterjord, 2023).

### Pathogen research, which is critical for pandemic preparedness, is targeted by malicious actors

Pathogen research is critical for effective pandemic preparedness, enabling early detection, development of diagnostics, therapeutics, and vaccines, and evidence-based response strategies (NIAID, 2021). The number of laboratories conducting pathogen research has increased since the first identification of SARS-CoV-2, the virus that causes COVID-19, in 2019. As of 2023, there were 51 operating Level 4 laboratories in 27 countries, representing about a twofold increase over the past ten years (Global BioLabs, 2023). Canadian laboratories that work with pathogens and toxins have made important contributions to domestic and international pandemic research, which makes them key targets for malicious activities (Cyber Centre, 2024a). During the COVID-19 pandemic, the Canadian Centre for Cyber Security and multinational technology companies detected an increase in the volume of threat activities against Canadian and foreign laboratories and other entities participating in pandemic response efforts (Cyber Centre, 2020). In July 2020, Canada, the United States, and the United Kingdom released a joint statement on the activities of APT29, a cyber espionage group targeting vaccine research organizations to misappropriate intellectual property (NCSC *et al.*, 2020). Researchers and research organizations continue to be targets of cyber threat activity for espionage and financial gain, resulting in the implementation of additional measures to safeguard sensitive research of concern (Cyber Centre, 2024a).

## 2.3 Open science

Governments support open science mainly for its promises to accelerate scientific progress and promote positive societal impact (EC, 2019; GC, 2020; UKRI, 2024a). At its core, open science ensures the implementation of an

internationally recognized legal principle: that people have the right to enjoy the benefits of scientific progress (UNGA, 1948, 1966; ISC, n.d.). In healthcare, for example, data-sharing among researchers can lead to more rapid innovation and discoveries, resulting in faster access to treatments or cures for rare diseases (Rubinstein *et al.*, 2020). Additionally, giving patients access to research means they can become more empowered in their care (TOH, 2021).

To this end, several countries, including Canada, enacted policies mandating that publications or other research outputs be shared (e.g., TBS, 2014; ISED, 2016; OSTP, 2022; cOAlition S, n.d.-a,-b). Within the Canadian government, the 2014 Directive on Open Government defined new objectives with regard to open data, which subsequently led to the Chief Science Advisor's 2020 Roadmap for Open Science that more comprehensively outlines responsibilities of federal departments and agencies concerning open science (TBS, 2014, 2018; GC, 2020). This roadmap spurred the creation of several coordinated but distinct open science action plans across various departments and agencies (e.g., DND & CAF, 2021; ECCC, 2021; StatCan, 2024d). In the panel's opinion, the implementation of these policies by the Government of Canada is critical for enhancing public access to intramural research and the consistent application of open science principles across the research ecosystem.

Open science, however, does not imply universal access; in practice, access is often limited and focused on particular aspects of research. Open-by-default policies do not grant unfettered access to raw data, and the unconditional availability of data and metadata for access and use is considered an exception rather than the default at a typical research data repository (CoreTrustSeal Standards and Certification Board, 2022). All researchers in Canada must comply with federal, provincial, and territorial privacy laws and respect the principle of Indigenous data sovereignty, which stems from the rights of Indigenous Peoples to self-governance and self-determination (GC, 1982; UN, 2007; OPC, 2018; CIHR *et al.*, 2022; FNIGC, n.d.). The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2) outlines additional considerations relating to confidentiality or other measures to restrict disclosure and access to potentially sensitive or personal data (CIHR *et al.*, 2022). Compliance with TCPS 2 is mandatory for institutions eligible to administer tri-agency funding and for researchers conducting tri-agency funded research (CIHR *et al.*, 2022). Within the federal government, researchers are urged to respect "privacy, security,

Open science does not imply universal access; in practice, access is often limited and focused on particular aspects of research

ethical considerations and appropriate intellectual property protection" despite pursuing an open-by-default posture (GC, 2020). Moreover, some open science advocates criticize open-by-default as a potentially imprudent paradigm with a narrow ethical justification, particularly given the power of emerging platform technologies such as AI (Spitale *et al.*, 2024).

### The Government of Canada's recent efforts to promote the uptake of open science have focused on responsible management and the sharing of data

A key component of Canada's shift to open science involves responsible storage, management, and sharing of research data, supported by the Tri-Agency Research Data Management Policy (RDM policy) (GC, 2021b; Moher & Cobey, 2021). This policy, adopted in 2021, requires action on behalf of institutions and researchers and encourages data-sharing if it is allowed under applicable ethical, cultural, legal, and commercial requirements (GC, 2021b) (Box 2.1). Adopting these actions can support both open science and research security by requiring consideration of responsible information-sharing.

## Box 2.1 Key elements of the tri-agency RDM policy

- **Institutional strategy:** All post-secondary institutions and research hospitals eligible to administer tri-agency funding must publish an RDM policy, which includes, among other things, "promoting the importance of data management to researchers, staff and students; guiding their researchers on how to properly manage data in accordance with the principles outlined in the Tri-Agency Statement of Principles on Digital Data Management, including the development of data management plans," and "providing, or supporting access to, repository services or other platforms that securely preserve, curate and provide appropriate access to research data."
- **Data management plans (DMPs):** Best practices in RDM should inform all research proposals submitted to the tri-agency, and some proposals must include DMPs that will be considered in the review process. DMPs should describe "how data will be collected, documented, formatted, protected and preserved; how existing datasets will be used and what new data will be created over the course of the research project; whether and how data will be shared; and where data will be deposited." DMPs should also assign

(continues)

(continued)

responsibility for managing data, describe succession plans, and outline limitations (ethical, legal, and commercial) on data.

- **Data deposit**: By the time of publication, federal funding recipients must store in a repository "all research data, metadata and code that directly support the research conclusions in journal publications and pre-prints that arise from agency-supported research." The chosen repository must ensure safe data storage, preservation and curation.

The policy also provides that institutional strategies, DMPs, and data deposits must advance the principle of data sovereignty with respect to "data created in the context of research by and with First Nations, Métis, and Inuit communities, collectives, and organizations."

(GC, 2021b)

According to Moher and Cobey (2021), successful implementation of the RDM policy in Canada depends on several factors, including:

- training and education of researchers—developing a core syllabus that could be tailored to different institutions and disciplines;
- funding for data-sharing—supporting researchers' efforts through grants and investments in data-sharing services;
- audit and feedback—implementing dashboards that monitor data-sharing rates and then establishing benchmarks;
- meta-science—evaluating progress across and within disciplines and the post-secondary research ecosystem; and
- career advancement—using alternative metrics when assessing researchers for career advancement.

This last factor is aligned with the recommendations of the San Francisco Declaration on Research Assessment (DORA), which is signed by more than 22,300 individuals and organizations, including CFI, Canadian Institutes of Health Research (CIHR), Natural Sciences and Engineering Research Council of Canada (NSERC), Social Sciences and Humanities Research Council (SSHRC), and Fonds de recherche du Québec (FRQ) (DORA, 2012; FRQ, 2020; NSERC, 2023). Otherwise, efforts made by researchers to share research data and materials may not be rewarded or recognized from a professional standpoint to the same extent as open-access publications (Moher & Cobey, 2021).

In the panel's opinion, research data management is an important element of research security, as it enables researchers to store and use data throughout the research process and, when appropriate, share it. Moreover, strong research data management practices directly advance the goals of recently adopted federal research security policies (Section 2.4) by providing researchers and institutions with the means to uphold research integrity (GC, 2024c).

### Before the adoption of the RDM policy, measures to encourage open science in publicly funded research have focused almost exclusively on open-access publications

Currently, the tri-agency policy requires that publications be open access within 12 months (ISED, 2016), although this approach is under review (ISED, 2023d). In alignment with broader international commitments to maximize the quality and impact of research, the FRQ is asking beneficiaries to provide immediate open access to peer-reviewed publications (CoARA, 2022, 2025; FRQ, 2022). Institutional open-access mandates may also exist in addition to those established by the research funder (e.g., SFU, 2023). Despite these policies, the participation of Canada's academic research community in open access is inconsistent (Moskovkin *et al.*, 2021; Simard *et al.*, 2022). Canada's track record in open-access publishing is poor in comparison to that of EU member states and other G7 members—approximately half of the articles published between 2015 and 2019 by authors in Canada are openly available (Paquet *et al.*, 2022; EC, n.d.-b). Other open science practices, such as clinical study registration and reporting of results, which are key to supporting evidence-based decision-making in medicine, are also not widely implemented in Canada (Alayche *et al.*, 2023).

> Strong research data management practices directly advance the goals of recently adopted federal research security policies

### Private companies rely on various mechanisms to limit access to research

For private R&D (including companies borne out of academic research), sharing access to research or research data proceeds differently, and the government lacks the levers of tying funding requirements to open-access policies. Access to research in the private sector involves incentives and motivations that are less well-defined than those of government-funded researchers. Knowledge, software, research results, and data are all critical, intangible assets for businesses, particularly in the tech marketplace (Asselin & Speer, 2019; Lamb &

Munro, 2020). Remaining competitive requires strategic decisions surrounding the disclosure and protection of these and other assets that comprise a company's IP.

Some economically valuable research outputs are kept confidential and considered trade secrets, which are a key component of IP strategy for businesses (WIPO, n.d.). Partnership agreements between academic researchers and the private sector can invoke trade secrets or confidentiality to make exemptions to open-data policies (Plomp *et al.*, 2019; MESR, 2021). Non-disclosure agreements are also commonly used to enforce confidentiality in the private sector (EC, 2022; van der Molen *et al.*, 2023). Moreover, the disincentive to share data in partnerships may be heightened due to legal repercussions for misappropriating trade secrets under major North American free trade agreements (Malone, 2021; Akhtar, 2024).

These factors do not always result in the private sector withholding research results unconditionally. Instead, some strategic considerations (e.g., potential monetization of research outcomes) can guide decisions to share openly (Pannier, 2023). In AI research, for example, some large technology developers espouse openness and publish vast amounts of software and data (e.g., Heikkilä, 2024), while their competitors pursue an opposite course due to perceived opportunity costs resulting from excessive transparency (Heaven, 2023; Pannier, 2023; Tiku & de Vynck, 2023; Yao, 2023).

## 2.4 Research security

In response to the growing number of security risks faced by Canada's research ecosystem, different orders of government have ramped up its research security efforts to manage the misappropriation and undesirable use of research generated in Canada.

### 2.4.1 Federal policy environment

While biosecurity has been a focal point of security efforts for several decades, in 2021 and 2024, the Government of Canada implemented two main policies—the National Security Guidelines for Research Partnerships (NSGRP) and the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC)—that leverage federal research funding in order to place limitations on research partnerships in diverse sensitive research areas.

### The STRAC policy prohibits those aiming to advance sensitive technology research areas from maintaining active affiliations with named research organizations

The STRAC policy, which came into force in 2024, introduced additional eligibility criteria for federally funded research partnerships. Research projects are ineligible for federal funding if they meet two criteria: (i) a member of the research team has an active affiliation with or receives funding and/or in-kind support from a foreign named research organization (NRO) "connected to military, national defence, or state security entities that could pose a risk to Canada's national security" (ISED, 2023e); and (ii) research is being advanced in one of the defined sensitive technology areas (ISED, 2023b). Although the requirements on affiliation, funding, and in-kind support apply to the entire research team, only researchers with named roles must submit an attestation on meeting the requirements of the STRAC policy (ISED, 2023f)—potentially leading to confusion about who is accountable and what is expected from other team members.

The STRAC policy defines the list of NROs and technology areas that it considers sensitive in order to provide guidance to researchers carrying out self-assessments when applying for federal research funding (ISED, 2023f). The list of NROs was developed by Public Safety Canada (PS) based on a number of disclosed and confidential indicators (PS, 2023). One disclosed indicator is if an institution publicly states it is conducting research for a foreign military or security agency. Private companies are currently excluded from the list, and other mechanisms, like the NSGRP, are used to manage potential risks in private sector collaborations.

The list of sensitive technology areas was developed by PS in cooperation with other federal departments and agencies and includes technologies that can be used by malicious actors to "degrade Canadian or allied security or defence efforts or enhance an adversary's security or defence efforts" (PS, 2023). These technology areas are:

- Advanced digital infrastructure technology
- Advanced energy technology
- Advanced materials and manufacturing
- Advanced sensing and surveillance
- Advanced weapons
- Aerospace, space and satellite technology
- Artificial intelligence and big data technology
- Human–machine integration

- Life science technology
- Quantum science and technology
- Robotics and autonomous systems

ISED (2023b)

Recognizing that these are broad subject areas, the STRAC policy also contains subcategories and examples to provide a degree of specificity for researchers (ISED, 2023b). For example, the category of life science technology includes two subcategories—biotechnology and medical and healthcare technology—which, in turn, contain more specific research areas covered by the STRAC policy (e.g., biomanufacturing, synthetic biology, gene therapy) (ISED, 2023b). This list doesn't apply to "ubiquitous and widespread" technologies, unless there is a concern that novel applications of such technologies can pose risks (PS, 2023).

The lists of NROs and sensitive technologies are evergreen and adapted to technological developments through ongoing efforts of several government departments and agencies (PS, 2023). In this dynamic landscape, the application of the STRAC policy requires a case-by-case analysis by researchers and post-secondary institutions. In 2025, the Government of Canada released a Sensitive Technology List (STL), which includes the same 11 categories of technology as found in the STRAC policy, but provides more detailed information and examples for each category. The STL is not directly related to research security policies, but it could be used to update future iterations of the STRAC policy (GC, 2025g).

### The NSGRP includes national security considerations in the creation, evaluation, and funding of research

In 2021, the Government of Canada released the NSGRP (ISED, 2021), which aims to protect Canada's research ecosystem from "foreign interference, espionage, and unwanted knowledge transfer that could contribute to advancements in military, security, and intelligence capabilities of states or groups that pose a threat to Canada; or disruption of the Canadian economy, society, and critical infrastructure" (ISED, 2023a). The NSGRP applies to a number of federally funded research programs, including, but not limited to, research partnerships supported by the tri-agency (ISED, 2023a). These include NSERC Alliance grants, CIHR Project Grant program, Tri-agency Institutional Programs Secretariat Canada Biomedical Research Fund (Stage 2); organizations funded through the Strategic Science Fund (e.g., Genome Canada); and all research funded through CFI, except the College Fund (Genome Canada, 2024a,b; NSERC, 2024b; CFI, n.d.-b). Although the exact timelines for applying the NSGRP to some CFI programs, including the Major Science Initiatives Fund, have not yet been determined, some research facilities have taken steps to

enhance research security in alignment with both the NSGRP and the STRAC policy (CFI, n.d.-b; CLS, n.d.; GlycoNet, n.d.).

The NSGRP covers more types of research security risks than the STRAC policy and extends to 11 sensitive technology research areas, as well as to other areas listed in Annex A, including critical minerals, critical infrastructure, large datasets, and personal data that "can be considered sensitive" (ISED, 2023a). Research funding applicants must submit a risk assessment form with their grant application if their funding opportunity falls under the NSGRP and they plan on conducting research with a qualifying partner (ISED, 2024a). What constitutes a qualifying partner depends on the funding opportunity, creating complexities and uncertainties for funding applicants (U of A, 2024a) (Table 2.1), though some harmonization is in progress.

**Table 2.1 Some examples of definitions of private-sector partner under the NSGRP, depending on research funder**

| Research funder | Definitions |
|---|---|
| Tri-agency | "Private sector partner organizations involved in the proposed research project, including industrial associations and producer groups" (NSERC, 2024b). |
| CFI | • "Has an active role in the research activities described in the proposal (e.g., sharing of intellectual property, providing expertise, actively participating in research activities, contributing financially to the research activities); or<br>• houses part or all of the research infrastructure; or<br>• contributes more than $500,000 to the infrastructure through a cash or in-kind contribution to any single item" (CFI, n.d.-b). |
| Genome Canada (funded through the Strategic Science Fund) | "A for-profit organization, or an organization that assists, supports, connects and/or represents the common interests of a group of for-profit, incorporated organizations, such as an industry association or a formal or informal consortium" (Genome Canada, 2024b). |

### Lists of dual-use items, sanctioned persons, and sanctioned entities limit research collaborations, as well as the transfer and sharing of technologies and research results

Federal restrictions on research are typically limited to lists, whether of individuals, institutions, or areas of research. These are subsequently referenced in various regulations. For example, to ensure biosecurity, the Government of Canada has adopted a list of security sensitive biological agents (SSBAs) and imposed licensing requirements and other security measures on facilities and researchers working with them (GC, 2009, 2024d; PHAC, 2023). Lists of dual-use items, sanctioned persons, and sanctioned entities limit research collaborations, as well as the transfer and sharing of technologies and

research results. These lists are adopted under the *Export Control List* (GC, 2021c), the *Human Pathogens and Toxins Act* (GC, 2009), the *Human Pathogens and Toxins Regulations* (GC, 2024d), the *Nuclear Safety and Control Act* (GC, 1997), the *Nuclear Non-proliferation Import and Export Control Regulations* (GC, 2010), and other laws and regulations.

Despite significant progress in the field of research security, these policies and approaches have limitations. Biosecurity measures, lists of dual-use items, and sanctioned persons and entities provide fragmented federal jurisdiction over research security (Wagner & Zaia, 2023). Moreover, research security policies that are attached to federal funding omit significant parts of the research enterprise funded through other sources, such as the private sector (Flagg & Arnold, 2021). The current approach is also insufficient to prevent the transfer of sensitive technologies—developed with public funding—to entities of concern through commercialization, thereby posing risks to national and economic security (SRSR, 2024). Regardless of the research area, advancements in R&D and the application of rapidly developing technologies such as AI and quantum may create new circumstances in which identifying sensitive research becomes challenging, and list-based approaches become outdated (Section 3.2.1).

### 2.4.2 Subnational initiatives

A growing number of related research security requirements have been imposed by provincial governments. The Government of Ontario has implemented its own research security measures attached to research funding (Gov. of ON, 2023). These measures establish risk assessment and mitigation procedures for all publicly funded research projects and require that applicants (including universities) disclose their international partnerships to the province (Gov. of ON, 2023, 2024a) (Section 4.1.2). Additionally, in Ontario, research security is emerging as a new accountability metric for provincial operational funding received by universities (e.g., U of T, 2025). Meanwhile, the Government of Alberta has ordered that the four comprehensive academic and research universities in the province (University of Alberta, University of Calgary, University of Lethbridge, and Athabasca University) pause agreements with China that involve graduate student research, visiting researchers, and post-doctoral fellows in sensitive research areas identified in Annex A of the NSGRP (U of A, 2024b). As part of the 2024–25 competition, Alberta's Research Capacity Program requires that applicants for some funding streams uphold measures to safeguard research (Gov. of AB, 2024). If these grants support inter-institutional projects, research security requirements apply to researchers from institutions outside Alberta. Divergent approaches such as these can

complicate the consistent implementation of research security measures across the country (UCalgary & U of A, 2023) (Section 5.1).

### Canadian universities have been ramping up research security efforts

Canadian universities have played an important role in the development of government research security policies. The Government of Canada–Universities Working Group on Research Security, first established in 2018, has been instrumental in developing the Government of Canada's Safeguarding Your Research Portal and the NSGRP (U15, 2023). Institutional policies on research integrity and responsible conduct of research have laid the groundwork for the development of risk management frameworks, policies, and practices, including those associated with international collaborations and policies for the protection of research data, research results, and IP (U15, 2023).

While research support services at universities have experience dealing with sensitive data and research, federal, provincial, and territorial policies encourage universities to adopt a broader geopolitical lens in their approach to research security (Owens, 2023a). To enhance existing research support services, universities have established high-level administration roles focused on research security and created research security units. These staff have been more heavily involved in vetting research proposals in sensitive technology areas and screening foreign research partners and international collaborations (Owens, 2023a). These efforts have been made possible through dedicated Government of Canada funding provided in Budget 2022 and allocated through the Research Support Fund to 51 universities in 2024–2025 (GC, 2024e,f). The allocation method—based on the amount of research funding received by post-secondary institutions from the federal government—has resulted in significant differences in capacity and subsequent approaches across institutions (GC, 2024e; TIPS, 2024). The establishment of new administrative offices and functions requires additional funding, particularly at small- and medium-sized universities, healthcare institutions and affiliated institutes, and at colleges and polytechnics (Section 5.2).

The panel acknowledges the real tensions between open science and research security while stressing that it is not a zero-sum issue. In Canada, policies governing data-sharing in the two areas of interest—pathogen research and ocean research—reflect the interconnectedness between open science and research security (Section 4.3.2). For example, the Canadian Biosafety Guideline: Dual-Use in Life Science Research acknowledges that the decision to communicate the results of research involving SSBAs is rarely clear-cut. A well-developed communication plan outlining what will be communicated, to whom, how, and when is essential for achieving a balance between openness

and the need to protect sensitive information (PHAC, 2018a). The Ocean Networks Canada Data Policy underscores a default position of openness with exceptions based on clearly defined security, ethical, or legal concerns, including personally identifiable information, Indigenous partnerships, military or national security concerns, endangered species protection, or sensitive technology (ONC, 2021a).

The uptake of open science may be low in Canadian academic research due to the relative absence of strong research security policies. In France, open science practices are comparatively more widely employed despite strict research security rules (Owens, 2023b; CNRS, 2024). Infrastructure and compliance measures, such as the French Open Science Monitor, may have contributed to boosting the uptake of open science among researchers (MESR, 2023; Owens, 2023b). Given that the majority of research is presumably not sensitive and that Canada lags in data-sharing, policy-makers should expect to make progress in both research security and accessibility while monitoring and disentangling true areas of tension.

3

# Identifying Sensitive Research of Concern

## Chapter findings

- Various risk factors are used to identify sensitive research, and a combination of those, as well as the use of additional tools such as lists, risk assessments, and specialized expertise, can further determine if sensitive research is of concern. Researchers, institutions, and governments share accountability and responsibility for these activities.
- Tension exists between researchers' desire for clear and delineated guidance on how to identify sensitive research (e.g., lists) and those of policy-makers and research security experts, who prefer dynamic and responsive assessments of sensitivity.
- The level of sensitivity of research may change throughout the research process; identification measures may be repeated prior to, during, and after each research phase, involving all actors in the research system in greater or lesser capacities at various stages.
- Institutional or regional expert committees to assess the sensitivity of research can be successful in offering a combination of domain and research risk knowledge, providing support to researchers. They can also be an additional mechanism to identify sensitive research throughout the research process.

The first step in operationalizing research security measures is identifying sensitive research and determining when it becomes of concern. This step is challenged by the rapid pace of development and diffusion of emerging technologies—which heightens prospective tensions—as well as by ongoing shifts in the geopolitical landscape (Kosal, 2020b). For every researcher's goal to publish a novel application, there could conceivably be a new avenue for misuse (e.g., DiEuliis & Giordano, 2017; Spitale *et al.*, 2024). The level of research sensitivity has implications for the level of openness and access to research outputs; determining where on the continuum of fully open to completely closed the research and data sit is essential, and this judgment is influenced by the sensitivity of research. Similarly, determining the point at which sensitive research becomes of concern is impacted by several factors (Section 3.1) and is influenced by documented risks, as well as the risk perception of the actors responsible for the identification of sensitive research. Recall, defining sensitive research as a type that is of concern requires analysis of whether it can be misappropriated or misused immediately or in the future, with minimal or no modifications (Section 1.2). Several of the factors for

identifying sensitive research discussed below (Section 3.1), when considered in isolation or in combination, can also indicate that research is of concern. Additional tools are available to help assess whether a research project is of concern (Section 3.2).

A growing variety of research activities are now subject to research security frameworks (e.g., ISED, 2023f; EC, 2024a), which require capacity to assess and manage risk in rapidly evolving contexts and in areas where it was previously not needed (Chapter 5). The current approach to identifying sensitive research involves several actors in the research ecosystem, including researchers, institutions, and governments. Research security frameworks have been developed to help determine where research falls on the spectrum of sensitivity.

A growing variety of research activities are now subject to research security frameworks, which require capacity to assess and manage risk in rapidly evolving contexts and in areas where it was previously not needed

Frameworks to identify sensitive research typically advocate for risk-based approaches that balance academic freedom and open science with research security, and therefore aim to avoid scenarios where researchers forego publication or avoid projects for purely precautionary reasons (MPG, 2017; CNRS, 2024). For instance, in the United States, the Federal Select Agent Program has seen the number of registered entities decline from 247 in 2019 to 226 in 2023 (HHS *et al.*, 2020, 2024). In the panel's experience, this drop may be due to the increased level of scrutiny and administrative burden that deters researchers from engaging in this type of research. Thus far, evidence on the impact of emerging frameworks in Canada is limited, but the NSGRP (Section 2.4.1) pilot found that approximately 4% of proposals processed over a one-year period warranted a national security assessment by partner agencies (ISED, 2023c). The panel notes, however, that without dedicated monitoring and tracking of the impacts of research security (and open science) directives, it is difficult to determine their effectiveness and best practices for implementation (Section 5.1).

Social sciences and humanities research is largely excluded from sensitive research policy in Canada. Nevertheless, data collected in these fields could be used nefariously

Social sciences and humanities research is largely excluded from sensitive research policy in Canada (with some exceptions, e.g., the advancement of AI tools to analyze population data), which instead focuses on

the advancement of technologies or risks associated with partnerships (ISED, 2023a,f). Nevertheless, data collected in these fields could be used nefariously (e.g., as a source of disinformation or propaganda, to track dissident behaviour) (Spitale *et al.*, 2024). Risks to researchers themselves—and their academic freedom—are also features of sensitive research in social sciences and humanities, in particular when researching topics associated with foreign state interference or influence (e.g., Harlan, 2019). The policy gap stemming from the exclusion of social sciences and humanities disciplines—explicitly or de facto—from existing research security frameworks has been raised in France, with a recommendation for their inclusion in some national research security policies (Gattolin, 2021). Moreover, methodologies and practices used within the social sciences (e.g., psychology, economics, sociology, political science) may be instrumental in designing and understanding evidence-based practices in research security (Dao *et al.*, 2024) and promoting uptake through institutional or cultural change (Huising & Silbey, 2018; Huising, 2019) (Section 5.4).

To address this gap, the definition of *sensitive research of concern* (Box 1.1) adopted by the panel encompasses threats to public health and safety, inclusive of privacy and ethics—not least of which are the rights expressed in UNDRIP, which asserts that Indigenous Peoples have the right to own and control information and data about themselves (Section 1.3). Researchers in the social sciences and humanities may already be aware of ethical or privacy risks, but not necessarily consider their research to be sensitive in terms of national security. In the panel's experience, for example, developing databases for health organizations requires addressing risks through security measures and platform design, and openness is constrained more by privacy and jurisdictional issues than by risks to national security. This tension complicates the identification of sensitive research.

Certain factors relating to potential risks can alert researchers, institutions, and governments that further analysis is needed to determine the level of sensitivity and whether the research is of concern

Certain factors relating to potential risks can alert researchers, institutions, and governments that further analysis is needed to determine the level of sensitivity and whether the research is of concern. Identification of some of these factors may immediately lead research to be recognized as sensitive and of concern (e.g., weapons research), while others require additional analysis or clarification through the use of various tools (e.g., as a component of risk assessment; Section 3.2). This chapter discusses some of these factors, as well as tools that can then aid the research community in

understanding the level of risk and next steps for safeguarding research at the appropriate level. These tools are applied to examples and scenarios in pathogen and ocean research, both in terms of how they are being used in Canada and how practices may be implemented in the future. They can be found throughout this chapter and the next in the boxes entitled *Application of measures*.

## 3.1 Factors that make research sensitive

A variety of factors can signal to researchers that certain types of research may be sensitive and warrant additional assessment to determine whether research is of concern, as well as the level of exposure to risk and potential mitigation strategies. For example, research partnerships with individuals or institutions outside of Canada are common and encouraged, yet they may be considered sensitive due to risks associated with potential bad actors, regardless of nationality. It is critical to note, however, that the level of sensitivity may be determined to be very low and only warrant safeguarding measures such as basic cybersecurity protections for all partners involved. Another factor is the direct threat to human health or safety; working with certain pathogens immediately signals that the research is of concern, and the researcher can consider the best ways to safeguard their research (Chapter 4).

The two research focus areas discussed in this report may be subject to several unique triggering factors. For example, pathogens research is sensitive because much of the work could negatively impact people if misused. The factors to gauge whether it is of concern and the level of appropriate safeguards are context-specific and may be determined by using tools such as risk assessments (Section 3.2.2). The risk assessment may require the researcher to think about the transmissibility of certain pathogens, which would then lead the research to be classified as both sensitive and of concern. Ocean research, as a broader and less clearly delineated field of study, is subject to different types of factors that indicate potential risks. For instance, the sampling frequency of certain signals may vary in sensitivity, where a low sampling rate is considered sensitive but not of concern (e.g., bottom hydrostatic pressure sensors monitoring tsunami waves), whereas a higher sampling rate may pick up activity that is sensitive in nature and may provide enough detail to classify the data as of concern (M. Paulson, personal communication, 2025). In both research areas, the assessment focuses on whether the research can be misappropriated or misused immediately or in the future, with no or minimal modifications.

Table 3.1 provides a range of factors that indicate research sensitivity, some of which may be broad and widely applicable, while others are more domain specific. These may provide the initial signal to a researcher that their research is (i) sensitive, (ii) sufficiently risky to also potentially be of concern, or (iii) certainly of concern when specific factors are combined. The panel notes that this table is not exhaustive, and many other factors may be used across the research ecosystem. Furthermore, these factors are not equivalent in their relative levels of sensitivity, and they vary depending on the context and project.

### Table 3.1 Sensitive research factors

| Factor | Rationale and applicability | Tools for identification |
|---|---|---|
| **Partnerships**<br>Situations where researchers are collaborating with individuals or organizations outside of their own institution or Canada. | Researchers can consider whether partners and their affiliates are subject to influence, interference, or control by malicious actors (including foreign governments), which may "pose a national security risk by using the research knowledge, technology, and intellectual property" (ISED, 2024a). | Lists (e.g., in STRAC)<br>Risk assessments (e.g., due diligence) |
| **Research concerning Indigenous Peoples**<br>UNDRIP states that Indigenous Peoples have the right to self-determination in all aspects of research that affects them, their knowledge, and their Lands (UN, 2007). | Researchers working with Indigenous people, or on the Lands of Indigenous Peoples, are required to consult and collaborate with the Indigenous communities or individuals concerned to ensure that research is being undertaken respectfully, ethically, and in line with the desires of the communities in question. | Specialized expertise (e.g., research ethics boards, research permits) |
| **Research on humans**<br>Any research funded by the tri-agency is subject to the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2) if it involves human participants or human biological materials (CIHR *et al.*, 2022). | Research identified under these conditions is subject to ethics board approval, which in turn may involve stipulations for safeguarding research. | Specialized expertise (e.g., research ethics boards, research permits) |
| **Geography**<br>Research taking place in a specific geographic location. | Research location may impart a certain level of sensitivity, regardless of the type of research and who conducts it. The Arctic, for example, is both the subject of increasing geopolitical tension as well as the homeland of many Indigenous Peoples. | Risk assessments |

(continues)

(continued)

| Factor | Rationale and applicability | Tools for identification |
|---|---|---|
| **Technology readiness level (TRL)**<br><br>TRLs are systematic metrics used to assess the maturity of a particular technology, ranging from fundamental research to commercial availability (JASON, 2024). | TRL assessments have been suggested to evaluate the potential impact of technologies at different stages of development on national security (EC, 2021a; JASON, 2024). High-TRL items or related knowledge may require additional safeguarding measures given the relative ease with which the threat or impacts of misuse might be realized. | Risk assessments |
| **Potential harmful applications of research**<br><br>Project-specific assessments to evaluate future harmful applications of research, such as dual-use potential or unethical applications (JASON, 2019; Gov. of New Zealand, 2020, 2022). | The potential impact of research on economic and national security (e.g., increasing the offensive military potential of foreign nations, weakening domestic defensive capacity) is often identified as a separate factor that should be considered during risk assessments (CNRS, 2024; NPSA & NCSC, 2024). | Lists, risk assessments, specialized expertise |
| **Large datasets, geospatial data, and personal data**<br><br>Researchers are encouraged to exercise extra care when working with large datasets and personal data (e.g., identifiable health or genetic data, biometric data, financial data, private communications) (ISED, 2023a).<br><br>Geospatial data may also be sensitive, in particular high-resolution data that may accurately identify sensitive objects (e.g., U.S. GAO, 2022). | Datasets "may be analyzed to reveal patterns, trends, and associations, especially related to human behaviour and interactions [that may have] ethical, commercial, or legal impact on the individual, domestic, or international level" (ISED, 2024a). There may also be potential ethical concerns arising from misuse of research data (GC, 2021d). | Risk assessments, specialized expertise (e.g., ethics review) |
| **Institutional or national strengths**<br><br>Institutions or nations with strengths in particular areas or disciplines may consider these areas to be sensitive, particularly for economic security. | Research areas where the institution or nation may have world-leading capacity, or that hold a particularly high value for other reasons (Gov. of Netherlands, 2022; VU Amsterdam, 2023). | Lists, risk assessments (e.g., asset analysis), specialized expertise (e.g., institutional review bodies) |
| **Risks to researcher safety**<br><br>Research that may result in harms to researchers, stemming from the topic of their research (e.g., violations of academic freedom). | Threats to academic freedom, involving research on topics that may be considered sensitive by certain governments (e.g., criticism of government policies) or in locations undergoing conflict, where researchers are at risk of physical harms or persecution (Gov. of Netherlands, 2022; Heathershaw *et al.*, 2022). | Risk assessments |

Some of the factors listed in Table 3.1 are broad but are intended to stimulate context-specific assessments that account for the nature of the research and its participants. These can be guided by information, resources, and case studies, providing the necessary tools for investigators to self-assess risks to their research programs (e.g., GC, 2021d,e,f) as well as risk exposure, which is influenced by factors ranging from participation in foreign talent or recruitment programs to failures in establishing effective training and compliance protocols for biosafety or cybersecurity (GC, 2024g).

### 3.1.1 Challenges for identifying sensitive research

#### Differences in risk perception and conflicting incentives complicate the role of researchers in identifying research as sensitive

Some identification criteria may not align with the incentives of grant applications. Asking researchers to objectively assess the future impact of their research could be challenging because the incentive to exaggerate the work's impact may be in tension with the desire to potentially avoid national security scrutiny. In the panel's view, training researchers to anticipate potential challenges and threats (Section 5.2) and then developing strategies to address them proactively (Chapter 4) can help ensure that research remains both innovative and secure.

Moreover, asking researchers whether their projects can be considered sensitive places the burden of identifying sensitive research entirely on researchers, who may not be aware of the broad potential risks associated with their activities (Kosal & Huang, 2015; Evans *et al.*, 2022). France, for example, largely exempts researchers from this activity and instead transfers responsibility for identification to specialized government bodies (CNRS, 2024). An additional challenge that can occur, in the panel's experience, involves situations where researchers may not be made aware of a known vulnerability, since disclosure of its existence presents a security risk and therefore is not shared. Increasing transparency and enhancing partnerships with academia, Indigenous governments and organizations, and the private sector are key goals for the Canadian Security Intelligence Service (CSIS), which may help to overcome this barrier in the future (CSIS, 2024b).

In addition to procedural challenges in this area, decisions surrounding the level of tolerable risk will be influenced by risk perception; discrepancies exist between real and perceived risks (Dao *et al.*, 2024). In the biosecurity context, risk perception has been shown to be both inconsistent and variable across the general population as well as among communities of experts (Engel-Glatter & Ienca, 2018; MacIntyre *et al.*, 2020). These issues impact the governance of

emerging technologies (e.g., AI; Brenneis, 2024) and contribute to challenges in consistently interpreting and managing risk. This also relates to research involving Indigenous partners, who may identify, perceive, and prioritize research risks differently. For example, the First Nations Data Centre On-Site Policies and Procedures Guide requires that researchers consider potential harms to communities, and privacy issues pertaining to groups rather than individuals (FNIGC, 2021, 2024). Unfamiliarity with the nature of harms to communities or collective rights could therefore raise tensions when considering research risks alongside economic, national security, or other risks.

### Factors for identifying sensitive research are constantly evolving, warranting re-assessment of research at every stage

Once research projects have been conceived, funded, and are underway, there is still value in conducting regular assessments of potential risks, especially when the participants or parameters of research change, or unexpected results arise. For instance, increased tension in a geographic area (e.g., the Arctic) or evolving political situations with partnering countries (e.g., the United States) can have knock-on effects for the likelihood and impact of certain risks to research, increasing its sensitivity and potentially making it of concern. Alternatively, some research that is considered sensitive may no longer be considered as such, and safeguards may become more relaxed or removed altogether. The sensitivity of research may therefore change throughout the research process, and identification measures benefit from ongoing review—it is important to consider that tools such as lists and risk assessments are essentially snapshots in time and may not reflect the risk landscape at every point in the lifespan of a research project.

Tools such as lists and risk assessments are essentially snapshots in time and may not reflect the risk landscape at every point in the lifespan of a research project

Additionally, different actors in the research system will play varying roles as the research progresses. While research is ongoing, top-down government oversight will become less engaged in the process, and researchers may be required to self-assess risks as their research progresses. Institutional bodies, such as expert committees or research security offices, may be called upon to provide support for researchers who require assistance adequately characterizing the sensitivity of their research throughout the research process.

## 3.2 Measures and tools for identifying sensitive research of concern

Factors indicating that research may be sensitive and of concern can be clarified, analyzed, and compared using specific tools. These tools can be standalone (e.g., lists addressing one aspect of sensitivity) or combined to fully explore the risk landscape. For example, the appearance of a research area on a critical technologies list may then require a risk assessment to determine the level of sensitivity and types of risks most likely to manifest, indicating whether or not the research is of concern. Three broad categories of tools for identifying sensitive research of concern are discussed below: lists, risk assessments, and specialized expertise mechanisms.

### 3.2.1 Lists

A common tool for helping researchers determine whether their research is sensitive or sensitive of concern is a list. Lists are often top-down approaches; what is included on a list is determined by a government or institution (through risk assessment processes of their own) and is then implemented by researchers or institutions, depending on the context. Lists reflect a range of sensitivity factors. Relationships with foreign jurisdictions are guided by export control, permitting, and sanctions lists. Lists may also be combined to indicate a higher level of concern. The STRAC policy, for instance, comprises two lists (Section 2.4.1); if a researcher is aiming to advance an area on the sensitive research list but not with a named research organization (NRO), then no further actions are required under the policy. Sensitive research of concern is signalled when two factors (advancing specific technologies and partnering with NROs) are combined, and the safeguarding measure is deterring the researcher from conducting this research by withholding funding.

#### List-based approaches are common across jurisdictions for identifying research that may pose harms to individuals and populations

In various contexts, lists are employed to provide accessible measures for identifying sensitive research: trade controls regulating dual-use goods, items, and research activities with sanctioned people and entities; lists of sensitive research areas, technology areas, or critical technologies (e.g., STRAC policy; Section 2.4.1); lists of entities or affiliations of concern; and lists of SSBAs, which are relevant to biosafety and biosecurity (GC, 1992, 2025f; Gov. of France, 2020; ISED, 2023f; BIS, 2024; Gov. of Australia, 2024; Gov. of New Zealand, 2024). A 2024 Parliamentary committee report (The Nexus Between Science and National Security in Canada: The Case of the National Microbiology Laboratory in Winnipeg) recommends expanding the list of NROs of concern and creating

an additional list of trusted jurisdictions with whom IP and research may be shared more freely (CACN, 2024), which would support open science principles. Canada already provides lists of countries that are exempt from export controls for certain goods (GC, 2021c), but this may be expanded to include provisions for rapidly advancing technologies, as has been reflected in amendments to export controls (GC, 2025h,i).

Working with pathogens and toxins on SSBA lists necessitates adhering to requirements for researchers and research facilities relating to licensing and security clearances (e.g., Gov. of Australia, 2013; PHAC, 2018a). While lists of dual-use goods and SSBAs are largely standardized pursuant to international non-proliferation treaties, other lists are tailored to address domestic security concerns. These lists, however, share some commonalities relating to the identified areas of research (e.g., emerging technologies) and the jurisdictions of affiliation of research partners (e.g., China, Iran, North Korea, Russia). Many allied jurisdictions have adopted lists of sensitive research areas or technologies, which vary in their specificity and enforceability. In Australia, for example, the List of Critical Technologies in the National Interest outlines some of the benefits and risks of the critical technologies and aims to coordinate and align the development of these fields within Australia and its governmental activities (Gov. of Australia, 2023). In Canada, receipt and retention of federal research funding from specified funding streams requires adherence to research security policies, including the STRAC policy (Section 2.4.1).

**APPLICATION OF MEASURES:**

## Lists for pathogen research

Canadian policies and guidelines specifically relating to pathogen and toxin research include the *Human Pathogens and Toxins Act* (HPTA) (GC, 2009) and the *Human Pathogens and Toxins Regulations* (HPTR) (GC, 2024d), as well as the Canadian Biosafety Guideline–Dual-Use in Life Science Research (PHAC, 2018a). The HPTA is meant to "establish a safety and security regime to protect the health and safety of the public against the [risks] posed by human pathogens and toxins" (PHAC, 2021), while the HPTR specify how PHAC will implement the HPTA and authorize controlled activities with human pathogens and toxins. These documents provide a list of SSBAs that are safeguarded through licensing and security clearances. Researchers apply for security clearance through PHAC to conduct certain types of pathogen research (a safeguarding measure discussed in Section 4.1.1).

(continues)

(continued)

**Roles and responsibilities:** "HPTA and HPTR apply to organizations and individuals conducting activities with human pathogens and toxins, [including] universities, public health laboratories, industry, hospitals, and diagnostic services for human and animal health" (PHAC, 2024b). They are maintained and enforced by PHAC.

**Stage of research:** For consideration and implementation in the research design phase.

**APPLICATION OF MEASURES:**

## Lists for ocean research

Outside of military research explicitly covered under the *Defence Production Act* and controlled goods regulations (GC, 1985b, 2016; PSPC, 2024), restrictions on ocean research in Canada originate in export control legislation and the STRAC policy, where several listed technologies may be applied to, or are directly concerned with, marine technology development (ISED, 2023b; GC, 2025f). The majority of those technologies are listed in the category 'advanced sensing and surveillance' and include technologies that "detect, measure or monitor physical, chemical, biological or environmental conditions and generate data or information about them" (ISED, 2023b). Of particular importance to ocean research are acoustic systems (such as single-beam, multibeam, and side-scan sonar), optical sensors (like cameras, LiDAR, and fluorescence sensors), electromagnetic sensors (e.g., magnetometers and sub-bottom profilers), as well as technologies for navigation, communication, and environmental monitoring (including CTD sensors, chemical analyzers, and underwater communication systems) (Sun *et al*., 2021). These technologies use acoustics to scan bodies of water, image the seafloor, and communicate, collect, or transmit data for the purposes of surveillance, exploration, and monitoring. The development of semi-autonomous or uncrewed marine vehicles is also on this list (ISED, 2023b). These sensitive technologies are of concern for national security, but they are also important for civilian and academic purposes.

**Roles and responsibilities:** The STRAC policy primarily governs researchers and organizations applying for tri-agency or CFI funding, though other individuals and organizations may also use it (e.g., Genome

(continues)

(continued)

Canada, 2024b). This excludes private companies and individuals developing and deploying these technologies independently—a common practice in certain marine technological development areas, in the panel's experience.

**Stage of research:** For consideration in the research design phase (pre-award).

Similar to the STRAC policy, the U.S. Department of Energy restricts collaborations in certain sensitive areas with researchers affiliated with China, Iran, North Korea, and Russia (COGR, 2023). The U.S. Department of Defense, however, is agnostic to research area and focuses on potential conflicts of interest and conflicts of commitment of researchers applying for fundamental research funding (DOD, 2023). The Australian Research Council (ARC) implements a different approach: if researchers apply for funding concerning technologies on the List of Critical Technologies in the National Interest, the ARC considers a range of factors to determine what risks may be present (e.g., foreign financial support, involvement in foreign talent programs, associations with foreign governments or militaries) (ARC, n.d.). If the ARC identifies a potential risk, national security agencies may become involved, and the host university's administration will be notified and required to provide a risk mitigation strategy or plan (ARC, n.d.). Within this framework, the ARC exerts some control over research security by having the ability to withhold funding for certain research until appropriate risk mitigation measures are proven (ARC, 2023).

At a provincial level, applicants to Ontario research funding programs are subject to research security review by the Ministry of the Solicitor General of Ontario (SOLGEN) (Gov. of ON, 2024a). SOLGEN may identify research projects as high risk if they involve collaborations or relationships that receive third-party funding or in-kind support (e.g., lab equipment, travel expenses, consultations) and the main applicant or any of the co-investigators are connected with "'hostile state actors' military, intelligence and national security apparatus, state-owned or influenced national research organizations, state-owned laboratories and enterprises … [or] sanctioned by the Canadian government" (Gov. of ON, 2024a). SOLGEN adheres to the two lists comprising the STRAC policy, but may also assess risks against additional resources, such as those provided by the United States and Australia, thereby further enhancing its risk evaluation (Gov. of ON, 2024a).

## Export control lists provide detailed guidance on materials requiring permits for export

Though researchers may participate in sensitive research within a given country, they are limited in the sharing and export of research outputs and technologies once research or development has been completed. Trade (or export) control lists are largely standardized and limit the export of dual-use goods and items identified in the international non-proliferation export control regimes (e.g., The Australia Group, 2023; WAS, 2023). In Canada, these lists are implemented through the *Export and Import Permits Act* (GC, 1985c) with details provided in the *Export Control List* (GC, 2021c), and through the *Nuclear Safety and Control Act* with details provided in the *Nuclear Non-proliferation Import and Export Control Regulations* (GC, 1997, 2010).

In addition to lists adopted pursuant to international agreements, countries implement economic sanctions and catch-all controls to limit the export of items not regulated under multilateral control regimes (EC, 2021b). France, for example, has adopted a list of quantum technologies and related processes subject to export control (Gov. of France, 2024). End-use, or catch-all controls are also in place for when there are "reasonable grounds to believe that such items may be intended for use in connection with a nuclear weapons program" (CNSC, 2014). Groups of goods and technologies listed as requiring export permits or licences in certain situations may be classified as dual use (as controlled through the *Wassenaar Arrangement*), munitions, nuclear non-proliferation (as controlled through the *Treaty on the Non-Proliferation of Nuclear Weapons*), nuclear-related dual use, missile technologies, chemical and biological weapons non-proliferation, and other miscellaneous strategic goods (GC, 2021c). Once goods or items have been identified as sensitive or dual use in these lists, an export permit or licence is required to engage in trade outside of Canada.

**APPLICATION OF MEASURES:**

### Export control lists for pathogen research

Research into pathogens and toxins is explicitly listed under Group 7 in the *Export Control List* and encompasses goods and technologies that Canada has agreed to control

> *... in accordance with the Guidelines for Transfers of Sensitive Chemical or Biological Items and the Common Control Lists, as amended from time to time, that are issued by the Australia Group to control the export of chemical and biological*

(continues)

(continued)

> *weapons; and…under the* Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction*, signed at Paris, France, on January 13, 1993, as amended from time to time.*
>
> (GC, 2021c)

**Roles and responsibilities:** All residents of Canada are bound by these rules. In practice, pathogen researchers are limited in their ability to share research findings and specimens with others, depending on the type of research they are undertaking.

**Stage of research:** Although researchers should be aware if their research is subject to export controls before beginning active research, these controls come into place in the post-research phase if the export of materials is requested.

### Lists can simplify the identification of sensitive research, allowing a greater number of individuals to participate in research security measures

Lists present several advantages. For example, academic researchers may appreciate the reduced administrative burden associated with cross-referencing their activities and partners to corresponding lists, in comparison to conducting risk assessments at varying levels of formality and rigour. Researchers in both pathogen and ocean research interviewed for this assessment expressed appreciation for lists as tools for simplifying processes around sensitive research identification, promoting clarity, and allowing for a more streamlined research process (D. Barclay and K. Subbarao, personal communication, 2024). Moreover, lists do not require researchers or administrators to have a strong understanding of risk assessment and potential for misuse. They can be used by administrators or staff to identify sensitive research at various stages in the process; for example, faculty grant officers may review grant applications to check against the STRAC policy as an additional step in the pre-award grant development process (S. Decrausaz, personal communication, 2024). However, as explained below, lists also have several downsides, leading some jurisdictions to use alternate or supplemental approaches (Gov. of New Zealand, 2020; Gov. of Netherlands, 2022; Leopoldina & DFG, 2022b).

### Some jurisdictions do not use lists because they can lead to a false sense of security and create vulnerabilities

Lists to identify sensitive research are not used across all jurisdictions. In the Netherlands, for example, lists of countries, partner organizations, or sensitive research areas are generally not used outside of the export control setting because they are viewed as flawed and problematic by decision-makers and research organizations alike (AWTI, 2022; Gov. of Netherlands, 2022; KNAW, 2023). By implying that research activities that do not intersect with lists are safe, lists can arguably contribute to a false sense of security (KNAW, 2023). In the panel's view, researchers who do not see themselves or their research in policy documents will not evaluate their research for sensitivity and risk in the same way that researchers whose work is mentioned or adjacent will, creating a vulnerability.

Listing criteria may also provide potential adversaries with details that may be used to circumvent security policies (PS, 2023), while lists carry the additional risk of fuelling discrimination against groups of researchers based on nationality (KNAW, 2023). Country-agnostic screening, as practiced in France, avoids stigmatization by requiring all researchers (French and international) to undergo security screening if working in certain sensitive areas (CNRS, 2024). As a compromise, some jurisdictions, including Aotearoa New Zealand, acknowledge that lists exist and can be useful resources, while encouraging researchers to use their own judgment (Gov. of New Zealand, 2020, 2022). Many of these drawbacks are most pronounced if lists are relied upon too heavily, but alternative uses of lists and changes to how they are populated present promising alternatives (Section 3.2.2). In the panel's view, Canada's heavy reliance on lists (e.g., the STRAC policy) puts it at risk of these drawbacks.

**APPLICATION OF MEASURES:**

#### Most areas of ocean research do not appear on sensitive research lists

Ocean research is one area where current lists may lead to a false sense of security for researchers and institutions. Although certain types of technologies appear in the STRAC policy (e.g., advancement of unmanned underwater vehicles), other areas of research and data outputs that are known to be somewhat sensitive (e.g., acoustics, fish tracking) do not (ISED, 2023b). While many of these research areas may not be considered of concern or pose immediate risks to human health,

(continues)

(continued)

some level of sensitivity may be warranted, in the panel's view, especially in certain geographic areas like the Arctic.

### Lists can become outdated due to rapid advancements in research areas, or by being too broad or too narrow at the outset

The level of detail used in a sensitive research list is an important factor in its effectiveness. For example, overly broad lists result in a level of ambiguity that may provide researchers with leeway to include or exclude research activities or outputs depending on their framing (JASON, 2024). In Canada, the STRAC policy may not adequately identify or provide clarity on the full scope of what research may be considered sensitive. For example, the list dictates that "of specific concern is the advancement of a technology during the course of the research" (ISED, 2023b). What constitutes *advancement* may be unclear, especially in areas where existing technologies are used in novel applications (e.g., side-scanning sonar in new regions) but may not be perceived as novel in and of themselves. In these situations, institutional research security offices, or specialized regional organizations, may be able to provide additional supports in navigating the process to identify sensitive research (PS, 2024a). The panel notes, however, that not all of these entities have achieved their full potential to date due to insufficient resourcing (Section 5.1).

In contrast, overly detailed lists can be unwieldy due to the amount of information needed to ensure a lack of ambiguity (JASON, 2024). Extensive efforts would be required to build and maintain a database in support of such detailed lists, along with consistent updates to ensure timeliness (JASON, 2024). Lists of this nature could also conceivably grow much longer based on the rapid rate of technological development (Hähnel, 2024). The rapid advancement of certain technologies further complicates the use of lists, which may quickly become out of date (KNAW, 2023). The STRAC policy is intended to be updated periodically to reflect technological advances and changes to the risk profiles of foreign institutions; any changes will only be forward-looking and not apply retroactively (PS, 2023; NSERC, 2025).

**APPLICATION OF MEASURES:**

### Multiple emerging technologies contributing to pathogen research present challenges to identification of sensitivity

A central challenge moving forward for measuring risks in pathogen research is the convergence of several emerging technologies and biological sciences, with implications for the identification of sensitive research (Himmel, 2023). Quantum technologies, and quantum computing specifically, are projected to accelerate computational tasks relating to biological processes and drug design (Gunashekar *et al.*, 2022; CCA, 2023b). Similarly, AI technologies can be combined with pathogen research to generate novel pathogens or change the virulence of pathogens in a targeted manner (Brockmann *et al.*, 2019). AI technologies present challenges for assessing risks and imposing appropriate standards for their use (Pouget & Zuhdi, 2024).

**Roles and responsibilities:** All actors in this system may be challenged by this issue, but researchers from discrete fields may be at a distinct disadvantage as they may lack the expertise to have a broad view of research security risks for collaborative multidisciplinary projects.

**Stage of research:** This challenge presents during the research design phase; however, researchers may also encounter it in the active research phase if new tools and technologies are incorporated into methodologies as they are developed.

## Periodically reviewed institutional lists avoid several drawbacks and can be more responsive to technological and research advancements

In lieu of foregoing top-down lists provided by the central government, institutional research security teams in the Netherlands are encouraged to generate internal lists of research topics, informed by risk assessment, to guide security activities (Gov. of Netherlands, 2022). This process involves conducting prized asset analysis to identify research areas where the institution may have world-leading capacity or hold a particularly high institutional value for other reasons (Gov. of Netherlands, 2022; VU Amsterdam, 2023). In the panel's view, identifying sensitive research topics at the institutional level and allowing for re-assessment as research evolves can avoid some of the aforementioned drawbacks of lists while still creating clarity for researchers and departments. In contrast, however, publicly identifying valuable assets may also draw the unwanted attention of nefarious actors, and runs the risk of becoming overly protectionist from an economic standpoint.

The U.S. Department of Energy does not rely exclusively on lists to identify potentially sensitive research (COGR, 2023; JASON, 2024). Instead, its subject matter experts conduct periodic assessments to evaluate the current state of progress in several areas of research associated with economic competitiveness, national security, and/or scientific leadership (e.g., batteries, quantum, AI) (JASON, 2024). Research in these areas is then categorized into three groups: fundamental and non–sensitive, potentially sensitive from an economic or national security standpoint, or requiring additional protective measures. This classification is used to restrict activities such as foreign engagements and travel, cooperative R&D agreements, and access to projects and data that involve countries of risk (China, Iran, North Korea, Russia) (COGR, 2023) (Section 4.2). NASEM[8] (2022) recommended the adoption of a similar approach across the U.S. federal government because it shifts the focus from critical technology lists in favour of strategically important classes of technology, which is better aligned with protecting U.S. national interests. JASON[9] (2024) also supports adopting a more flexible and dynamic approach to identifying potentially sensitive research based on its potential applications, TRLs, and direct and predictable national security impact. Although lists present numerous downsides, the above approaches can improve their usefulness as a resource rather than a decision–making tool.

**APPLICATION OF MEASURES:**

## Prized asset analysis for ocean research

Several academic institutions in Canada house departments or faculties focusing on ocean research. These entities may be considered important assets if they are world-renowned or perform research of vital importance to Canada and its participation in international initiatives such as ocean observation networks (DFO, 2022; CIOOS, n.d.-a,-b; GOOS, n.d.). Listing areas of institutional strength and conducting risk analyses for each of these sensitive areas can aid in determining appropriate safeguarding measures for national security, the safety of staff, and academic integrity (Gov. of Netherlands, 2022). As the sensitivity of research may change over time, these institutional lists benefit from being periodically reassessed (Gov. of Netherlands, 2022).

(continues)

8 The National Academies of Sciences, Engineering, and Medicine in the United States.

9 JASON is an independent group, established in 1960, that advises the U.S. federal government on defence, science, and technology (DOD, 2022).

(continued)

**Roles and responsibilities:** Institutions are responsible for conducting asset analysis and may be supported by governments providing resources to implement risk analyses.

**Stage of research:** Throughout the research lifecycle.

### 3.2.2 Risk assessments

Once the researcher has identified a factor that indicates sensitivity, risk assessments are helpful tools for determining the level of sensitivity of research, how factors interact with one another, and whether sensitive research is of concern. Risk assessment is a "formal, systematic process for estimating the level of risk in terms of likelihood and consequences for the purpose of informing decision-making" (PS, 2010). The goal of risk assessment is to provide a clear understanding of potential risks and their likelihood, along with their possible impacts on desired outcomes (PS, 2010). Once risks are identified, appropriate risk mitigation measures can be implemented (Chapter 4). However, risk assessments may require those utilizing them to have a better understanding of potential risks to research security to do an assessment; in comparison, the use of lists does not require a similar level of knowledge.

#### The core principles for assessing risk are adaptable to diverse contexts

Risk assessments help researchers and institutions identify instances where their research and collaborations may be of concern, but assessments vary in terms of their specificity. While some assessments can follow detailed guidelines asking researchers to consider additional risk factors (e.g., technological readiness levels, criteria for determining institutional autonomy) (Gov. of Australia, 2021; JASON, 2024), others rely on researchers' judgment to identify risks based on broad guidelines (e.g., anticipated risk) (Gov. of New Zealand, 2020). Publicly available information provides Canadian researchers with guidance to conduct their own assessments (ISED, 2022b), though institutions and administrators may also have responsibilities in this space. In the Netherlands, for example, the National Contact Point for Knowledge Security "can share information and expertise available in the ministries and services of the central government and consult on possible mitigation measures that could be taken" (Gov. of Netherlands, 2022).

The governance of these various risks typically follows a set of widely used processes that can be aligned with international standards (e.g., ISO, 2018). The

specific terminology used in these processes (and how they are implemented) varies according to application area and is reflected in differences across federal government departments and agencies that employ risk-based oversight (e.g., PHAC, 2018a; PMRA, 2024; PS, 2024b). The factors indicating potential sensitivity discussed in Section 3.1 may serve as a precursor to, or a major component of, risk assessments, depending on the discipline.

Despite the influence of context on the methodological details of risk governance and its role in decision-making, risk assessment is ubiquitous and plays a key role in the identification of sensitive research. To account for differences in application areas, the first step of risk assessment typically involves a context-setting exercise (PS, 2012). This defines the themes of interest for risk assessment, the individuals or groups involved, and any relevant historical considerations. This step can, for example, define the scope and relevant timelines for risk assessment (Verga, 2013).

**APPLICATION OF MEASURES:**

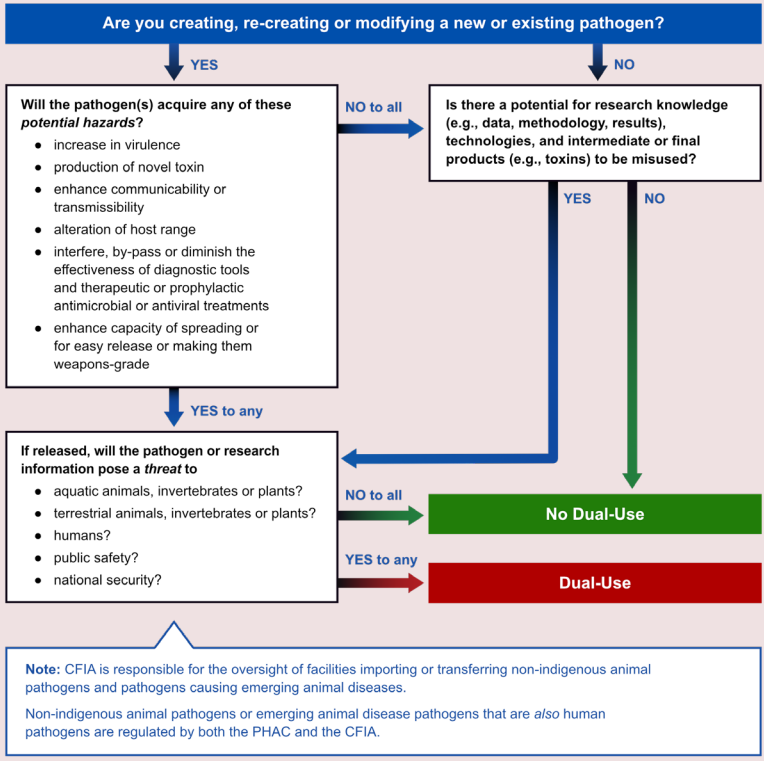
## Biosafety risks in the Canadian Biosafety Guideline

The Canadian Biosafety Guideline details how to identify pathogen research with dual-use[10] potential by offering a decision tree asking several questions about the characteristics of an organism or toxin, including harmfulness, novelty, modification risks, and misuse potential (Figure 3.1).

(continues)

10 Dual-use research and dual-use research of concern are the terms used in this box instead of the broader sensitive research of concern due to the specificity of language in the PHAC process. PHAC defines dual-use potential as "qualities of a pathogen or toxin that allow it to be either used for legitimate scientific applications (e.g., commercial, medical, or research purposes), or intentionally misused as a biological weapon to cause disease (e.g., bioterrorism)" (PHAC, 2018b).

(continued)






## Figure 3.1 PHAC process for identifying the dual-use potential of research

This decision tree outlines how research subjects (e.g., pathogens) and outputs might lead to, or exacerbate, hazards. Pathogen and toxin research uses dual use and dual-use research of concern as preferred terms instead of sensitive research.

CFIA – Canadian Food Inspection Agency
PHAC – Public Health Agency of Canada

The panel notes, however, that there are other risk factors beyond those listed in this decision tree, including unique production methods and the potential to re-create previously extinct pathogens. PHAC recommends that research found to have dual-use potential based on the questions in Figure 3.1 be subject to a risk assessment to evaluate if existing biosafety and biosecurity measures are adequate (PHAC, 2018a).

(continues)

(continued)

**Roles and responsibilities:** PHAC is charged with creating these risk assessments, while researchers are responsible for implementing them.

**Stage of research:** Research design phase.

### Risk assessments may guide partnerships in research collaborations

Outside of lists, risk factors associated with foreign partnerships may also be addressed through risk assessment processes to be completed by researchers or institutions. Risk assessments may include conducting due diligence of partners based on publicly available information and expert advice, researchers formally disclosing conflicts of interest and commitment when applying for funding, and determining the institutional autonomy of research partners. Publicly available information, such as current and past affiliations and projects, and disclosed research funding sources, may suggest existing or potential conflicts of interest (Gov. of New Zealand, 2020; Gov. of ON, 2023; ISED, 2024a). In some instances, addressing legislative complexities associated with due diligence processes requires cross-departmental input within research institutions, including "legal, governance, finance, international office, development office, and information technology" (Marwaha *et al.*, 2023). Threat assessments conducted by intelligence agencies may also offer relevant information for conducting due diligence with potential partners and better understanding the nature and scope of threats (e.g., cybersecurity threats) (CSIS, 2024b; Cyber Centre, 2024c). In the Conducting Open Source Due Diligence for Safeguarding Research Partnerships guidance, ISED lists several foreign companies that may accelerate and supplement due diligence activities (ISED, 2022c). The panel notes, however, that relying on foreign due diligence tools may be at odds with Canadian values and priorities, particularly in the face of dynamic geopolitical circumstances.

### Participatory risk assessment processes capture valuable perspectives outside of researchers or governments

Among the key justifications for having researchers self-assess risks and other aspects of sensitive research is the sense that researchers possess a deeper understanding of their subject area than external assessors do (SIGRE, 2024). However, researchers may struggle to assess the sensitivity of their activities due to a combination of factors, including a lack of training, insufficient time, the breadth of risks to assess, and bias. Under these circumstances, it may be beneficial to consider efforts undertaken in participatory risk assessment,

which could potentially aid in identifying hazards and strategies for effective engagement with impacted communities regarding risk (Stirling *et al.*, 2018). Where evolving technologies can impact citizens or patients, involving communities and other knowledgeable parties (e.g., healthcare practitioners) in the assessment may offer a more thorough account of risk tolerances and sensitivities, leading to a more robust decision-making process. Participatory exercises such as workshops and multi-criteria mapping within risk assessments have been effective in informing governance frameworks around emerging biological technologies (see review in Stirling *et al.*, 2018). Leveraging existing relationships could be an avenue forward for this method of risk assessment; the community liaison committee at the Vaccine and Infectious Disease Organization (VIDO) provides education and resources to the public about its research (VIDO, 2025), while simultaneously conveying community concerns and questions back to VIDO (V. Gerdts, personal communication, 2025).

### Expert committees can bolster existing processes for risk assessment and create communities of practice, provided conflicts of interest are appropriately managed

In some jurisdictions, independent committees of experts have emerged. These share similarities with research ethics boards but are tasked with identifying sensitive research. For example, Stanford University has established an Ethics and Society Review Board (ESR) in order to assess AI research for its potential impacts on society (Bernstein *et al.*, 2021). This process is a required step for researchers to receive institutional funding. Surveys and interviews conducted with researchers who went through the ESR process found that "58% felt that it had influenced the design of their research project, [and] 100% are willing to continue submitting future projects to the ESR" (Bernstein *et al.*, 2021).

At a national scale, the German Research Foundation (DFG) and National Academy of Sciences Leopoldina (Leopoldina) introduced a framework in 2022 aimed towards both researchers and research institutions to oversee "security relevant research" (Leopoldina & DFG, 2022b). Specifically, they define security-relevant research of concern as "scientific work that has the potential to produce knowledge, products or technologies that can be directly misused by third parties to cause significant harm to human dignity, life, health, freedom, property, the environment or peaceful coexistence" (Leopoldina & DFG, n.d.-a). This research is classified as of concern because the potential damage is significant and misuse can be foreseen as immediate. Notably, the guidance recommends that academic institutions create specialized research ethics committees known as Kommissionen für Ethik sicherheitsrelevanter Forschung

(KEFs) tasked with overseeing security-relevant research and helping to designate it of concern (Leopoldina & DFG, 2022b; Jakob *et al.*, 2024). Each institution recruits experts to serve on a KEF that can provide advice to other researchers. The KEF is empowered as an institutional decision-making body in the area of security-relevant research through internal policies and regulations (Leopoldina & DFG, 2022b). Should an institution lack the necessary capacity or resources to host a KEF, coalitions may come together to create KEFs to serve multiple institutions while sharing resources. KEFs are further supported by the DFG and Leopoldina Joint Committee on the Handling of Security-Relevant Research, which shares experiences and acts as a point of contact (Leopoldina & DFG, 2022b).

A central responsibility of the KEF is to carry out assessments of research, which consist of a self-assessment directed to the researcher, followed by assessments by the KEF (Leopoldina & DFG, 2022a). KEFs ask questions regarding the nature of the research and its objectives, participants, and sponsors. This line of questioning concerns several ethical areas relating to benefits and risks (intended or unintended) and asks whether researchers possess the knowledge or resources to make informed and accurate decisions from an ethical standpoint (Jakob *et al.*, 2024; Leopoldina & DFG, n.d.-b). The KEF then poses a series of questions to inform a conclusive assessment, querying researchers on potential misuses of research, need for re-assessment by the KEF, compatibility with constitutional principles, ethical considerations, and whether risks can be adequately reduced by the imposition of proposed conditions (Leopoldina & DFG, 2022a).

The KEF approach potentially fills gaps that may be overlooked in processes strictly reliant on self-assessment. Jakob *et al.* (2024) caution, however, that if the necessary expertise for an assessment cannot be found within a KEF, outside experts from other KEFs or elsewhere must be included in the assessment, which can raise issues related to confidentiality or data protection. This model elicited concerns among members of the panel regarding conflicts of interest, given that fields where sensitive research is taking place tend to be highly competitive—at both the institutional and individual level. Moreover, as an opt-in process, the KEF model relies on a culture where security is taken seriously; impediments or delays to research are accepted as legitimate and necessary on this basis, which implies the establishment of a particular institutional research culture (Jakob *et al.*, 2024). The panel also emphasizes the commensurate need for resources and supports to minimize any potential administrative burden and significant time costs arising from a KEF-type review, particularly for researchers who may already be reluctant to engage in mandatory review or research. Limited time to apply for grants would impact

the effectiveness of these types of committees, as any elongation of the application process would likely be negatively received by researchers. Nevertheless, the creation of such committees could assist in building communities of practice, particularly at regional levels, since some considerations of risks (and threats) may be more relevant than others when it comes to research security (CNRS, 2024), and since capacity and resources may be strongly divergent across institutions (UNL, 2024), particularly in Canada (TIPS, 2024).

Expert groups, such as KEFs, present both opportunities and drawbacks, but their inherent multidisciplinarity and the involvement of experts specializing in ethics are assets in navigating the sensitivity of research. KEFs offer an alternative to other national research security frameworks investigated by the panel, which primarily focus on natural and applied sciences due to their direct link to technology as well as their potential economic significance (e.g., SGDSN, 2018; Gov. of Australia, 2023; ISED, 2023b; Gov. of United Kingdom, 2024; UKRI, 2024b; ASIO, n.d.).

**APPLICATION OF MEASURES:**

### Institutional review boards for ocean research

As with prized asset analysis, institutions with existing strengths in ocean research could employ review committees to help determine the level of sensitivity of research, as well as appropriate safeguards if it is deemed to be of concern. These committees may be comprised of researchers within institutions but may also benefit from the participation of other actors in the ocean research system (e.g., representatives of private industry, fisheries, governments, and coastal Indigenous communities). In situations where institutions lack sufficient capacity to undertake internal reviews, regional or national organizations could be leveraged or formed to serve in this capacity for a greater number of institutions with similar strengths. For example, the Oceans Research in Canada Alliance (ORCA) has a mandate to coordinate ocean science and technology efforts and acts as a forum to share information and discuss priorities within ocean research (ORCA, 2022). ORCA, whose secretariat is housed within Fisheries and Oceans Canada (ORCA, 2023), may be able to support a review body to help researchers and institutions assess sensitive research and avoid internal competition among researchers that may stymie efforts to establish internal review boards.

Institutional review committees could also assess research sensitivity in certain geographic areas, such as the Arctic. Northern Indigenous

(continues)

(continued)

sovereignty and the right to research, as well as escalating geopolitical tensions are factors that add complexity to identifying sensitive research in this area. Institutions and organizations conducting research in the Arctic may benefit from establishing committees to help identify risks and formulate strategies on how best to mitigate risks and account for this complexity. The panel cautions, however, that any bodies dictating how research is being conducted in the North (especially when considering risks to northern populations) should be led by northerners, and by northern Indigenous Peoples more specifically, where capacity exists (CCA, 2023a).

**Roles and responsibilities:** Institutions and regional or national research organizations.

**Stage of research:** In the research design phase, with the possibility for re-assessment during the active phase.

### 3.2.3 Specialized expertise

Specialized expertise external to the researcher or institution conducting research is another measure that can identify the relative sensitivity of the research in question and designate it as of concern. In situations where responsibility for identifying sensitive research is shared with partners who have specialized knowledge, these partners may flag certain research processes or outputs as sensitive in all phases of research.

#### Indigenous Knowledge Holders are best placed to identify sensitive information when it concerns them or their Lands

In cases where researchers are working in collaboration with, or on the Lands of, Indigenous Peoples, there are situations where Indigenous Knowledge Holders may bring their expertise to bear in the identification and protection of sensitive information. For example, in the case of surveying coastal erosion processes in the Inuvialuit Settlement Region, a federal researcher from the Geological Survey of Canada relied on the knowledge and guidance of members of the local hunter and trapper committees to aid researchers with respectfully interacting with graves that were eroding out of the landscape due to

Indigenous Knowledge Holders may bring their expertise to bear in the identification and protection of sensitive information

permafrost thaw and ground subsistence (D. Whalen, personal communication, 2025). Once research outputs and data are identified as sensitive, data management or governance plans created in accordance with the protocols of Indigenous communities and rights-holders (in the research design phase) may be implemented to determine the appropriate level of access and sharing, as a component of the safeguarding process (Section 4.2.4).

### Research partnerships with military actors may require the identification of sensitive data by specialists with classified knowledge

In situations where research data outputs are known to be potentially sensitive, partnerships with relevant organizations may be put into place to identify sensitive data in real time. For example, the panel heard from several ocean researchers whose work was overseen by the Canadian Armed Forces and DND, either through memoranda of understanding (MOUs) or funding agreements.

**APPLICATION OF MEASURES:**

#### Screening of ocean research data by military partners

Ocean Networks Canada (ONC) operates a network of acoustic sensors off Canada's coasts, producing data that are made publicly available online (ONC, n.d.-a,-b). However, some data may be of importance to national security and are thus screened by military partners for sensitive content, a process governed by an MOU between ONC and DND (M. Paulson, personal communication, 2025). Data collected that are deemed sensitive are retained indefinitely, to prevent access of the sensitive data from potential bad actors. Non-sensitive data are returned to ONC for archiving and open-data use (M. Paulson, personal communication, 2025) (Section 4.3).

**Roles and responsibilities:** Researchers, institutions, and specialized expertise holders (e.g., the military) can make agreements in advance, and potentially as a condition of funding.

**Stage of research:** While agreements to conduct this screening are established during the research design phase, screening occurs as data are being collected during the active phase.

## Some journals have editorial policies to review submitted manuscripts for sensitive research of concern potential

While relatively few journals have published policies on reviewing sensitive research, in several cases, journal editorial boards have engaged in this type of review (Musunuri *et al.*, 2021). In these situations, editors, special committees convened by journals, government bodies, reviewers, and authors participate in the identification of the level of sensitivity or risk of publishing research and make decisions on how best to safeguard it (e.g., redacting certain information, rejecting submissions outright. The rapid proliferation of pre-prints during COVID-19 increased concerns about the lack of review for dual-use potential, a process that can happen during publication but is largely circumvented through pre-prints (Musunuri *et al.*, 2021). Several pre-print servers created screening processes for dual-use potential prior to submission, though authors may choose not to submit to the pre-print servers offering this utility (Yoshizawa *et al.*, 2023).

**APPLICATION OF MEASURES:**

### DURC[11] potential assessment by journal publishers

Certain journals use the expertise of their referees to identify DURC potential; in response to recommendations from the U.S. National Science Advisory Board for Biosecurity, journals overseen by the American Society for Microbiology introduced a questionnaire in 2007 asking referees to assess whether submissions involved "experiments of concern" (Casadevall *et al.*, 2015). More recently, these journals have employed a more formalized process for dealing with DURC utilizing three stages: screening, discussion, and decision (ASM Journals, 2021). The screening process (i.e., identification phase) involves several key actors and steps. First, self-declaration of sensitive content by authors may be found in the submission cover letter, alerting editors and reviewers to consider biorisk in their reviews. Editorial staff then consult the U.S. Select Agents and Toxins List, and search for key phrases relating to increased virulence, transmission, or related concepts that would trigger enhanced scrutiny of the manuscript. Should a manuscript be identified as DURC, the editorial staff then moves on to the next stages of discussion and decision to determine the level of access and publication (i.e., sharing) for the manuscript (Casadevall *et al.*, 2015; ASM Journals, 2021).

(continues)

11 DURC is used instead of the broader sensitive research of concern due to the specificity of language in this process, as it concerns pathogen research.

(continued)

**Roles and responsibilities:** Journal editorial staff are implicated in this measure.

**Stage of research:** In the post-research phase, as a condition of publication.

### Indigenous research partners have the right to determine how research outputs are shared

Indigenous Peoples have the right to dictate how research and information about them and their Lands are used, including how these are shared once collected (Section 1.3). MOUs, access and benefits sharing agreements, and data governance plans can all be established prior to the start of research to set roles and responsibilities regarding how research outputs are treated upon the completion of research (CCA, 2023a). In these situations, decision-making lies with Indigenous communities or individuals (e.g., Elders, members of hunter and trapper committees); these identify the sensitivity of certain information and then dictate how it may be shared in order to adequately protect it (Section 4.3.3).

**APPLICATION OF MEASURES:**

#### Identification of sensitive research by Indigenous community partners

Researchers working with coastal Indigenous communities or on the Lands and waters of Indigenous Peoples should be conscious of sensitivities associated with ocean research. For example, in a situation where a researcher maps the locations of breeding or spawning grounds for fish, local Indigenous communities who rely on these resources may identify this information as sensitive for its cultural significance and thus wish to control access to this information to avoid negative impacts such as overfishing (M. Hoeberechts, personal communication, 2025).

**Roles and responsibilities:** Indigenous Peoples and Knowledge Holders can exercise their right to protect information about themselves and their Land. Researchers should be aware of the rights codified in UNDRIP and their responsibilities to conduct research in a respectful way.

(continues)

(continued)

**Stage of research:** Agreements and relationship-building should be conducted prior to the start of research, with communication on potential risks and outcomes throughout the active and post-research phases.

4

# Safeguarding Sensitive Research of Concern

## Chapter findings

- Measures to safeguard sensitive research of concern are interconnected and contextual, and they need to be revisited throughout the research process to maintain a balance between openness and security.
- Implementing and complying with measures to safeguard sensitive research of concern are shared responsibilities among researchers, institutions, and governments.
- Measures to safeguard sensitive research of concern focus on the first two phases of the research process: research design and the active research phase. There is a lack of clear guidance on responsible data-sharing and publication of research results in the post-research phase.
- The principles of self-governance and self-determination uphold the right of Indigenous Peoples to decide how to safeguard sensitive research of concern. A lack of support and resources as well as the dominance of non-Indigenous research institutions prevent Indigenous Peoples from fully realizing these rights.

The second step in the operationalization of research security measures is safeguarding sensitive research once it has been deemed to be of concern. The application of these measures depends on a range of factors, including the nature of the research project (e.g., subject matter, methodology, research participants), funding sources, and research partners. These measures can be considered best practices for safeguarding the research enterprise more broadly and applied to both sensitive research and sensitive research of concern while balancing open science and innovation.

The measures discussed in this chapter are organized according to the stages of the research process—the research design phase (Section 4.1), the active research phase (Section 4.2), and the post-research phase (Section 4.3). These measures are interconnected and must be used consistently to be effective. Despite various mechanisms that can be applied to people, institutions, and research projects, the implementation of safeguarding measures is often fragmented and left to the discretion of individual researchers and institutions. Moreover, existing approaches focus on the first two phases of the research process, leaving researchers and institutions with little guidance on sharing data and communicating research results. This chapter concludes by discussing considerations that can help all actors of the research ecosystem determine

their roles and responsibilities in the implementation of safeguarding measures (Section 4.4).

## 4.1 Research design phase

In the research design phase, researchers make important decisions about their project, including identifying the research question and methodology, potential partnerships and collaborations, and funding sources. Researchers, institutions, governments, and funders can safeguard sensitive research of concern from misuse and misappropriation by adopting measures that prevent malicious actors from getting access to data, knowledge, information, and IP at the outset of the project.

### 4.1.1 Screening of researchers

Immigration, Refugees and Citizenship Canada (IRCC) conducts a security assessment of all foreign nationals (including professors, visiting researchers, and students) applying to study or work in Canada in any field or discipline (PS, 2024c). This assessment is focused on determining whether the applicant has been involved in criminal activities. Based on the results of this assessment, some researchers may be declared admissible to Canada, while others may be subjected to a comprehensive security screening that involves the Canada Border Services Agency (CBSA) and the Canadian Security Intelligence Service (CSIS) (PS, 2024c). One of the goals of the comprehensive review is to determine if the applicant presents a national security risk (and a risk to sensitive research) based on several factors, including their education, employment history, and research interests, as well as open-source information on the hostile activities of foreign countries (e.g., FC, 2023a,b). As a result of the review, some researchers may be declared inadmissible to Canada under the *Immigration and Refugee Protection Act* for a number of reasons, including being a national security risk or engaging in espionage (GC, 2001; PS, 2024c). This review, however, represents a snapshot in time and cannot account for researchers' changing circumstances and motivations, due, for example, to external pressures and threats (HC & PHAC, 2022). These risks highlight the need for a periodic review of security measures and security clearances, if applicable (HC & PHAC, 2022). Regardless of the results of security reviews completed by IRCC, CBSA, and CSIS, those actively affiliated with certain named research organizations (NROs) and working in sensitive research areas identified in the STRAC policy are ineligible for tri-agency funding in those areas (ISED, 2023f).

**APPLICATION OF MEASURES:**

### Security screening of ocean researchers

Foreign ocean researchers applying to work and study in Canada are subject to security assessments and may also be subject to comprehensive security screenings by IRCC, CBSA, and CSIS. Ocean researchers and organizations can refer to the STRAC policy to avoid collaborations with researchers affiliated with NROs (ISED, 2023f).

Unlike Canada, some jurisdictions have formally incorporated research security considerations into the immigration review process and moved to targeted immigration screenings for researchers from certain countries working in sensitive research areas. For example, the Government of the United Kingdom has introduced Academic Technology Approval Scheme certification requirements for foreign students and researchers from certain countries who are working in sensitive research areas (Gov. of United Kingdom, 2025). A Government of the Netherlands plan to introduce a screening process for non-EU nationals working in high-risk areas has been criticized for its potential to cause discrimination and immigration processing delays (De Bruijn, 2023; Gov. of Netherlands, 2025; Sharma, 2025).

**APPLICATION OF MEASURES:**

### Security screenings of people working with SSBAs

In addition to security checks performed by IRCC and its partners, the *Human Pathogens and Toxins Act* (HPTA) establishes special security procedures for all researchers (Canadian and foreign) undertaking projects with SSBAs (GC, 2009). Researchers must obtain security clearance under the HPTA (PHAC, 2024c). The application for HPTA security clearance is submitted to PHAC and includes information on places of residence, employment and education history, and spouse or common-law partner, as well as a criminal records check. Foreign nationals must provide additional documentation, including a copy of their curriculum vitae and foreign police record checks (PHAC, 2024c). The Evaluation of the *Human Pathogens and Toxins Act* and Regulations Framework completed by PHAC and Health Canada in 2022 raised issues regarding security clearance criteria (HC & PHAC, 2022). Biological Safety Officers suggested expanding the list of who should have a

(continues)

(continued)

security clearance—that is, beyond those working with or having access to SSBAs—"as well as increasing the level of scrutiny prior to issuing [a] security clearance for foreign nationals." The evaluation also suggested implementing continuous vetting of issued security clearances (typically valid for five years), noting that circumstances can change over time (HC & PHAC, 2022).

### 4.1.2 Security review of research proposals

Research proposals may be subject to additional security screenings before they reach peer review. For example, under the NSGRP, a risk assessment is conducted independently of the merit review and consists of the following steps:

1. *Preliminary administrative review.* The granting agency reviews the applicant's risk assessment form to ensure it is complete and conducts its own risk assessment based on publicly available information.
2. *Additional administrative review.* Applications with potential or identified risks are referred for a more detailed screening by the granting agency's Risk Assessment Committee, which considers the following: (i) the sensitive nature of research (per Annex A of the NSGRP) and (ii) whether "one or more private sector partner organizations were identified from open-source information to be associated with, or originating from, organizations or countries that are subject to sanctions, and/or associated with criminal or ethical concerns" (NSERC, 2024b).
3. *Merit review.* The granting agency proceeds with a merit review, but the risk assessment form submitted by the applicant and the results of the Risk Assessment Committee's review are not shared with peer reviewers.
4. *Review of some applications by security agencies.* Following a successful merit review, some applications flagged by the granting agency's Risk Assessment Committee are referred to PS for a national security assessment that may involve CSIS and the Communications Security Establishment Canada. PS may consult other departments (e.g., Global Affairs Canada) to consider additional pertinent factors, such as the economic and diplomatic consequences of funding the application.

5. *Funding decision*. The granting agency considers the results of the national security assessment and merit review to make the funding decision. Successful applicants are required to implement the risk mitigation plan described in their funding application and, in some cases, additional risk mitigation measures. Applicants who were denied funding based on the results of the national security assessment can request additional information from the granting agency and the Research Security Centre.

(GC, 2025j)

Between July 2021 and July 2022, NSERC used the NSGRP to review applications submitted to the Alliance grants program (ISED, 2023c). Out of 1,158 submitted applications, 48 (~4%) were subject to in-depth security screenings, and, of those, 32 (or ~2.5% of all applications) were rejected due to security concerns. These applications involved private sector partner organizations that had "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" (ISED, 2023c).

**APPLICATION OF MEASURES:**

### Security review of research proposals in ocean research

An ocean researcher applying for tri-agency funding (e.g., NSERC Alliance grant) must submit a risk assessment form with their grant application if their funding opportunity falls under the NSGRP and they plan on conducting research with a qualifying partner (e.g., private sector organization). The goal of this risk assessment form is "to identify and assess potential risks that research partnerships may pose to Canada's national security" (ISED, 2024a). A research proposal will be subject to a risk assessment conducted independently of the merit review. Although the NSGRP policy applies only to some publicly funded research, other organizations that fund ocean research may use it as guidance for conducting security reviews of research proposals based on open-access sources.

## The Research Security Guidelines for Ontario Research Funding Programs have a broader scope than the NSGRP and the STRAC policy

The Research Security Guidelines for Ontario Research Funding Programs (ORSG) apply to research collaborations funded through the Ontario Research

Fund (Gov. of ON, 2024a). The Government of Ontario's approach to research security is partially aligned with the federal STRAC policy (Gov. of ON, 2024a). However, the ORSG is broader in scope than the STRAC policy and the NSGRP; it requires that all named researchers in all funding applications submit an attestation form acknowledging that they comply with the ORSG (Gov. of ON, 2024a,b). These requirements apply regardless of the research area and affiliations (Gov. of ON, 2024a). Another difference is that the STRAC policy considers only active affiliations with research organizations of concern at the time of the application and for the duration of the grant (ISED, 2023f). The ORSG, however, considers collaborations within two years preceding the submission of the proposal and for the duration of the proposed project. Such collaborations include, but are not limited to, "co-authorship, co-publication, co-hosting of international conferences, joint research, or joint funding recipients, … a memorandum of understanding, partnership, joint venture, joint funding, joint degree/exchange program, graduate student supervision, visiting scholar, or participation in a foreign funded talent program" (Gov. of ON, 2024a). It is important to consider these differences if researchers participate in projects funded by both the federal government and the Government of Ontario. It is possible that some projects will comply with federal research security policies but may be considered high risk under the ORSG (UVic, 2024).

### A security review of certain research proposals is required by U.S. legislation

In the United States, there have been changes to the merit review of some projects funded by the National Science Foundation (NSF) due to security concerns mandated under the *CHIPS and Science Act of 2022*, which notes that "a number of emerging areas of research have potential … safety, and security implications that might be apparent as early as the basic research stage" (Gov. of United States, 2022b). The NSF has been examining how to best incorporate "ethical, social, safety, and security considerations into … the merit review process" to mitigate "the potential harms of scientific research" (NSF, 2024a). This review is in addition to other research security requirements imposed on the recipients of federal research funding (including the NSF and the National Institutes of Health) under federal policies and guidelines (NSTC, 2022; COGR, 2024).

**APPLICATION OF MEASURES:**

### Licences under the HPTA

In pathogen research, an additional layer of security and safety review applies to people and organizations proposing to conduct research activities[12] with human pathogens and toxins identified as risk groups two, three, and four (PHAC, 2024d). Such research requires a licence under the HPTA. Licence terms and conditions depend on the pathogen's risk group and the SSBA status of the toxin. A facility wanting to do research on pathogens falling under several risk groups and SSBAs will require several licences (PHAC, 2024d). Prior to getting a licence, applicants are also required to prepare biosafety and biosecurity action plans (PHAC, 2021).

## 4.1.3 Bans and preliminary approvals of research partnerships and collaborations

The governments of Canada and Ontario can refuse to fund research partnerships and collaborations that do not meet research security requirements (Section 4.1.2). However, the government's refusal to allocate research funding does not ban such partnerships and collaborations because bans and limitations do not have the same legal effect as government orders or legislation. Because higher education is administered by the provinces and territories (GC, 1982), respective governments can use mechanisms other than funding to require that the higher education sector exercise greater caution in international collaborations, or even pause or stop some of them.

For example, in 2021, the Government of Alberta ordered the four comprehensive academic and research universities in the province (University of Alberta, University of Calgary, University of Lethbridge, and Athabasca University) to pause any new or renewed partnerships linked to the Chinese government or ruling Chinese Communist Party in order to ensure such partnerships adhere to strict risk assessments and due diligence procedures (Chase, 2022). In 2022, these universities were allowed to resume "low-risk agreements" with China, though limited to arrangements for "undergraduate student mobility and transferability" and "corporate training opportunities" (SRSR, 2024). In 2023, colleges and research universities in the province were asked to pause only those agreements with China that involve graduate student

12 Defined broadly as "possessing, handling, using, producing, storing, permitting any person access, transferring, importing, exporting, releasing, abandoning, disposing" (PHAC, 2024d).

research, visiting researchers, and post-doctoral fellows in sensitive research areas identified in Annex A of the NSGRP (U of A, 2024b).

**APPLICATION OF MEASURES:**

### Research partnerships and collaborations among pathogen research facilities

"Work involving pathogens in Canada may require compliance with international, national, and provincial laws and guidelines" (PHAC, 2025a), which can impose limitations on international partnerships and collaborations (e.g., export controls) (GC, 2024h). Regulated facilities also use internal policies and directives, non-disclosure agreements, and training to safeguard their research (PHAC, 2024e). Facilities can use the STRAC policy as guidance to avoid collaborations that pose security risks. In addition, pathogen researchers applying for federal funding for projects that involve the application of life science technology (as identified in the STRAC policy) cannot collaborate with researchers affiliated with NROs (ISED, 2023b) and must comply with applicable legislation that covers broad topics, including research security.

## Some jurisdictions require preliminary government approvals on collaborations with foreign research institutions

Governments in foreign jurisdictions have been exploring and applying various regulatory approaches to address the security risks of research partnerships, including introducing stricter rules than Canada and imposed preliminary approvals for collaborations with foreign research institutions. In France, research institutions conducting activities covered under the *Regulation on the Protection of the Scientific and Technical Potential* must have their partnership agreements approved by the Ministry of Higher Education and Research (Pannier, 2023). In Australia, public universities must notify the Minister for Foreign Affairs before entering a partnership arrangement with a foreign organization (Gov. of Australia, 2020). The minister can ban the partnership if they determine that a foreign university lacks institutional autonomy based on one or more legislatively defined criteria:

(a) *a majority of the members of the university's governing body are required, by a law or the university's governing documents, to be members or part of (however described) the political party that forms the foreign government;*

> *(b) education provided or research conducted at the university is required, by a law or the university's governing documents, to adhere to, or be in service of, political principles or political doctrines of: (i) the foreign government; or (ii) the political party that forms the foreign government;*
>
> *(c) the university's academic staff are required, by a law or the university's governing documents, to adhere to, or be in service of, political principles or political doctrines referred to in paragraph (b) in their teaching, research, discussions, publications or public commentary.*
>
> (Gov. of Australia, 2020)

Some organizations and researchers met this system of legislatively imposed limitations and approvals on research partnerships with resistance and criticism (Morris, 2020). As noted by Universities Australia (2024), the legislation defines "arrangement, foreign entity and institutional autonomy" too broadly, placing an unnecessary reporting burden on universities. Moreover, it does not provide for a mechanism to appeal the decision of the minister (Universities Australia, 2024). Differences in legal systems and cultures need to be considered when assessing the extent to which foreign approaches are appropriate in a Canadian context.

### 4.1.4 Security provisions of research cooperation agreements

Researchers can mitigate security risks at the outset of a project by including relevant provisions in cooperation agreements with their research counterparts. Cooperation agreements can establish rules regarding the use of data and infrastructure, confidentiality, licences and transfers, registration of property rights, warranties, liability, applicable law, dispute resolution, and an exit clause for non-compliant partners (Leibniz Association, 2021). However, researchers must be aware that some jurisdictions "have laws or practices that compel entities and individuals to be subject to direction from their governments to provide Canadian information, research knowledge, technology, and its resulting intellectual property" (ISED, 2023a). In such cases, contractual provisions are largely unenforceable, making partnerships risky and beneficial only to one party.

### 4.1.5 Ethics review, research permitting, and licensing of Indigenous research

The principles of Indigenous self-determination and self-governance, codified in UNDRIP, guide Indigenous research (see definition in Box 1.1) and signify that Indigenous Peoples have the right to determine how to identify and then safeguard sensitive research of concern (UN, 2007). This right is fully realized

when Indigenous Peoples are equitable participants in the research process (ITK, 2018; GC, 2019a). In Canada, there is a lack of ethics reviews and research licensing mechanisms that support community-led and community-centric measures for safeguarding sensitive research of concern (CCA, 2023a).

### Ethics reviews and research licensing mechanisms do not fully uphold the rights of Indigenous Peoples to self-determination and self-governance

The Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2) contains considerations for those receiving tri-agency funding for research involving First Nations, Inuit, and Métis (CIHR *et al.*, 2022). However, the National Inuit Strategy on Research has explicitly stated that "companion ethical guidelines do not exist for research involving wildlife and the environment" (ITK, 2018). The system of research permitting and licensing administered by territorial governments and, in some instances, Indigenous communities (e.g., Nunatsiavut Government Research Advisory Committee, Ittaq Heritage and Research Centre) partially addresses the shortcomings of ethics reviews in this respect (CCA, 2023a; IHRC, n.d.; NGRAC, n.d.). The purpose of the process is to ensure a rights-based approach to safeguarding sensitive research of concern:

> *Coastal erosion research that doesn't involve humans is not subject to institutional ethics review. Still, researchers need to get a research permit from the Inuvialuit Settlement Region if they are conducting research on their Land. Similarly, physical data collected for geological research may be important to the community for security reasons. The system of research licensing exists so that the researcher remains accountable to the community.*
>
> (D. Whalen, personal communication, 2025)

Although licensing and research permits represent an important shift in influence over how Indigenous research is conducted, these processes are limited due to the insufficient capacity of Indigenous communities and governments "to review or engage with incoming research" (CCA, 2023a). For example, in the Arctic, "short timeframes, staffing limitations, duplication of processes at the territorial level, and a lack of contextual understanding about the North by Southern researchers have posed problems for effective and timely review by Indigenous organizations" (CCA, 2023a). Moreover, in the panel's opinion, additional mechanisms and resources are necessary to protect Indigenous data from misuse by non-Indigenous researchers during the active research phase and after the research project ends.

## 4.2 Active research phase

During the active research phase, researchers collect data, conduct experiments, make observations, and perform other activities to gather information necessary to test their hypotheses and answer the research question. At this stage, managing access to physical facilities and data—through controlled entry, cybersecurity, and travel restrictions—is crucial for safeguarding sensitive research of concern. Under the STRAC policy, research teams need to monitor their collaborations and partnerships during the active research phase (ISED, 2023f). Continuous monitoring of the research project by researchers and, if applicable, Indigenous Peoples is necessary to assess whether the implemented safeguarding measures are appropriate.

### 4.2.1 Controlled access to research facilities

Controlled access to research facilities is a critical and commonly deployed measure to safeguard sensitive research of concern that applies throughout the research process (COGR, 2023; EC, 2024b; JASON, 2024). While controlled access to research facilities, security clearances, and other restrictive measures may prevent some researchers from participating in experiments, clear rules around physical security and cybersecurity can also enable sharing and collaboration by creating a safe environment where researchers can freely exchange knowledge. "In aerospace technology research, security clearance is necessary to work on some research projects funded by DRDC and other government departments. Having clear rules around access to different parts of the laboratory allows researchers who do not have necessary security clearance to continue working on fundamental research" (P. Ferguson, personal communication, 2024).

**APPLICATION OF MEASURES:**

#### Controlled access to pathogen research facilities

It is common for public and private research facilities conducting pathogen research to establish different access levels to different parts of the facility (e.g., GC, 2009, 2024d; Gov. of Australia, 2024). Access requirements established in the Canadian Biosafety Standard (CBS) are informed by the need-to-know principle, which "restricts access to specific areas, regulated materials, and related assets … to individuals who need it as part of their job responsibilities" (PHAC, 2024f). Only people who "have a legitimate reason or authorization based on their job

(continues)

(continued)

responsibilities may access specific areas and related assets" (PHAC, 2024f). The CBS distinguishes between limited access and restricted access (PHAC, 2022):

- *Limited access* is permitted to authorized personnel and authorized visitors through operational means (e.g., supervision by authorized personnel) or using a physical barrier.
- *Restricted access* is permitted to authorized personnel using a physical barrier. Restricted access requirements apply to parts of the facility designated as containment zones and SSBA zones.

### 4.2.2 Cybersecurity

Whole-of-organization cybersecurity strategies that set out policies, standards, roles and responsibilities, digital identity management, measures for addressing vulnerability and managing threats, training and awareness programs, and business continuity planning can all help research institutions mitigate cybersecurity risks (UFIT, 2021). Shankar and Drake (2022) distinguish between institutional and research cybersecurity. They define the latter as a subset of institutional cybersecurity that applies "cybersecurity to research in a manner that accelerates research while limiting risk to the research mission." To be successful, a cybersecurity research program needs to be designed with the researcher and research mission in mind, reduce the cybersecurity and compliance burden on the researcher, and ensure security throughout the research process (Shankar & Drake, 2022).

**APPLICATION OF MEASURES:**

#### Cybersecurity at the Ocean Tracking Network

The Ocean Tracking Network (OTN), funded by CFI, includes infrastructure such as "acoustic and satellite transmitters, receiver lines, data storage capacity, and various physical oceanographic equipment." Data collected using this infrastructure are stored in a database. OTN has developed the following documents to support the preservation and stewardship of ocean data: a data management plan; a data decommissioning plan; and a cybersecurity plan that lists data resources and cyber assets, outlines risks and mitigation strategies, and sets out data control mechanisms.

(OTN, 2024)

Since the beginning of the COVID-19 pandemic, the Canadian Centre for Cyber Security (Cyber Centre) has observed a large volume of malicious activities against Canada's research organizations, including research laboratories (Cyber Centre, 2024a). The digitalization of research and the use of integrated information technology systems to conduct experiments with pathogens and toxins have made research laboratories easy targets of cyber interference (Cyber Centre, 2024a). Despite issues identified by the Cyber Centre, the CBS, and other policies regulating research facilities working with pathogens and toxins do not contain cybersecurity requirements applicable to all licensed facilities.

**APPLICATION OF MEASURES:**

### Cybersecurity requirements for containment level 4 facilities

PHAC is planning to introduce additional cybersecurity requirements for containment level 4 facilities in 2026; currently, there is one such facility—the National Microbiology Laboratory located at the Canadian Science Centre for Human and Animal Health in Winnipeg, Manitoba (GC, 2019b; PHAC, 2024f, 2025b). As of 2024, the Vaccine and Infectious Disease Organization (VIDO) is developing another level 4 facility in Saskatoon (VIDO, n.d.). Level 4 facilities will be required to implement a cybersecurity plan, policies on the use of digital devices, and a system for labelling, working with, and limiting access to sensitive information (PHAC, 2024f).

## 4.2.3 Travel policies

In Canada, one of the main documents guiding researchers' international travel is the Travel Security Guide for University Researchers and Staff developed by the U15 Group of Canadian Research Universities and Universities Canada (U15 & Universities Canada, 2019a). This country-agnostic and non-legally binding document contains a number of recommendations on how researchers can enhance both personal and cybersecurity while travelling abroad, including:

- "Do not travel with unnecessary documentation (contact lists, electronic files, etc.) or devices. Before you travel, carefully consider what data you need. Bring the minimum.
- Encrypt and transfer data onto a separate external storage device and keep it with you at all times while traveling. Keep data passwords separate from the media.

- Do not let your devices out of your sight at any time during your travel. If this happens, assume that the equipment has been compromised.
- Do not plug an unknown device, including USB keys, cameras or digital picture frames, into any of your equipment. Should you find it necessary to plug an external device into your equipment for presentation purposes at a conference, you should consider that your device has been compromised.
- If possible, do not access cloud data storage sources while travelling. If access to cloud storage is necessary, be sure to only do so on personal and secure devices.
- If your device is lost or stolen, notify your IT department immediately.
- Refrain from talking about sensitive parts of your research or potential future research in public places, or with contacts you have just met.
- Monitor the progress of associations, particularly new relationships and connections with foreign nationals and refrain from offers of personal companionship while travelling."

(U15 & Universities Canada, 2019a)

CSIS has also issued a research security guide addressed to businesses, industries, and academic institutions (CSIS, 2020). The guide contains a broad range of recommendations on mitigating risks to personal safety and cybersecurity arising from foreign intelligence, terrorism, and economic threats while preparing to go abroad and during international visits. It covers such topics as protection of personal and sensitive information when applying for a visa, vigilant behaviour at airports and hotels, and cybersecurity (CSIS, 2020). Several universities in Canada have also established travel security policies that outline offices responsible for training, registration, and communication with researchers travelling abroad (e.g., uOttawa, 2022; HEC Montréal, 2023).

The Government of the United States has introduced legally binding foreign travel security requirements on federally funded research organizations (NSTC, 2022). Research organizations must establish foreign travel policies for faculty and staff. Such policies can include a travel record and, if necessary, travel authorization and pre-registration requirements, security training and digital security assistance (NSTC, 2022).

### 4.2.4 Monitoring of research by Indigenous Peoples

Monitoring of Indigenous research by Indigenous Peoples ensures they maintain ongoing control over how their data are stored, processed, and shared throughout the research process (ITK, 2018; FNIGC, n.d.). In some cases, such monitoring has been formalized. For example, the Government of Canada's

Northern Contaminants Program, which was established to reduce contaminants in wildlife species, enables communication between researchers and Indigenous communities through Regional Contaminants Committees (GC, 2024i). In the United States, Tribal Institutional Review Boards controlled by Tribal Nations monitor and review research on the community's behalf (Around Him *et al.*, 2019). Formal systems of Indigenous monitoring of active research phases could be expanded in Canada, but they require sufficient "resourcing and capacity consistent with the values of the Indigenous Peoples concerned" (CCA, 2023a).

**APPLICATION OF MEASURES:**

### Labelling of ocean data by Indigenous people

Data-labelling systems controlled by Indigenous Peoples can also support continuous monitoring of the active research phase in compliance with the principle of data sovereignty (ONC, 2023). In 2023, Ocean Networks Canada (ONC) and the Canadian Integrated Ocean Observing System (CIOOS) launched a labelling tool for datasets developed in collaboration with Indigenous coastal communities. Communities can create and apply a customized label to a dataset by adding "provenance information and contextual metadata (including community names), protocols, and permissions for access, use and circulation." This labelling system allows for transparent but controlled accessibility of data in compliance with the principles of CARE (Collective benefit, Authority to control, Responsibility, Ethics) for Indigenous data governance (ONC, 2023). These principles advance the cultural security of Indigenous data and help ensure that Indigenous Peoples control them and benefit from sharing them (Carroll *et al.*, 2021; GIDA, n.d.). Some researchers believe that the CARE principles represent an important foundation for working with Indigenous data and that they will evolve and mature as they are applied in Indigenous communities (Carroll *et al.*, 2021).

In the absence of formal research monitoring mechanisms, researchers can rely on guidelines co-developed with Indigenous communities (e.g., the Ocean Frontier Institute's Indigenous Engagement Guide) as well as culturally appropriate community engagement (e.g., community presentations, posters, videos and films, radio shows, project summaries, brochures) to support continuous and accessible reporting of research findings to communities (ITK & NRI, 2007; OFI, 2022). Community feedback can help researchers identify sensitive or controversial aspects of their research before publication (ITK &

NRI, 2007). "Being accompanied by a member of the hunters and trappers organization while doing cliff erosion imaging helped us ensure that we dealt with their data in a culturally secure way. Some images were never published due to their sensitivity and significance to the community" (D. Whalen, personal communication, 2025).

## 4.3 Post-research phase

The post-research phase of the research process is focused on knowledge mobilization tactics that can accelerate the uptake and implementation of outputs. Responsible approaches to the publication of outputs and data-sharing (e.g., through self-imposed restrictions or external review) can help researchers advance open science and maximize the benefits of sensitive research of concern while ensuring that it remains out of the hands of malicious actors.

Responsible approaches to the publication of outputs and data-sharing (e.g., through self-imposed restrictions or external review) can help researchers advance open science and maximize the benefits of sensitive research of concern while ensuring that it remains out of the hands of malicious actors

### 4.3.1 Self-imposed restrictions on publication and data-sharing

Researchers rely on various knowledge mobilization methods, including publications and presentations, to share research findings with the broader public and accelerate the implementation of research outputs (CCA, 2024b). Not all research results, however, can or should be shared publicly (e.g., with those not involved in the project or lacking security clearance). Because research results alone, without detailed descriptions of used data and methodology, can pose significant risks or cause damage in some cases, researchers are encouraged to assess the possible consequences of publishing at the outset of the research project and continuously evaluate these risks throughout the research process (PHAC, 2018a; Leopoldina & DFG, 2022b). Sometimes researchers may be able to edit, redact, or otherwise limit access to research data without damaging the overall ability to publish (NPSA & NCSC, 2024). According to Inglesby (2024), however, this option is often problematic because "any attempts at redaction or removal of results in life sciences have provoked scientific firestorms in the past … Journals will not likely agree to be involved in this kind of redaction and the science community has itself harshly criticized scientists who tried to do this in the past." As a last resort, researchers may also consider delaying the publication of results or

not publishing it at all; however, decisions not to publish should be carefully weighed against the applicable research funding policies, and the principles of responsible conduct of research, open research, and free exchange of information (MPG, 2017; NSERC, 2018; PHAC, 2018a; GC, 2022b).

### 4.3.2 External pre-publication review of research findings

The pre-publication review of research findings may be required by the terms and conditions of research contracts, particularly when sensitive research of concern is funded or approved by government departments and agencies or private funders (Shea, 2006). "Aerospace technology is a sensitive research area. When research is privately funded, the pre-publication review of papers by the funder can be included in the conditions of the research contract" (P. Ferguson, personal communication, 2024). Laws and regulations provide clearer guidance on goods and technology transfers than they do on data-sharing and publication of research results (GC, 2025f) (Section 3.2.1).

**APPLICATION OF MEASURES:**

#### Publication of ocean research

In ocean research, restrictions on the publication and sharing of data may be imposed on a case-by-case basis (e.g., through research contracts and by the principle of data sovereignty; Section 4.3.3); the panel and the interviewed experts are unaware of policies or regulations limiting the open sharing of ocean data. CIOOS's national ocean data platform works with data producers on a case-by-case basis to address sensitivities around their data (CIOOS, n.d.-c). OTN treats all "animal morphology information and any ongoing locational information" to be restricted data by default (OTN, 2024). It allows researchers to request a two-year embargo (that can be extended on a case-by-case basis) on publishing animal tagging metadata due to its sensitive ecological nature (OTN, 2024). Most data collected from deep ocean and coastal water observatories operated by ONC are available free of charge in near real-time for anyone to use. Notably exempted from this rule are some seismic and hydrophone data that are screened by the Canadian and U.S. navies for national security reasons; these may be diverted prior to archiving (ONC, 2021a) (Section 3.1).

**APPLICATION OF MEASURES:**

## Publication of pathogen research

Policy documents issued by PHAC do not contain legally binding guidelines on how to, and who should, carry out pre-publication review of data and papers on pathogens (PHAC, 2018a). The Canadian Biosafety Guideline–Dual-Use in Life Science Research (the Dual-Use Guideline) provides that every research project should be reviewed "for dual-use potential during the planning stages, throughout the course of the project (including when there are unexpected results), and prior to the use or dissemination of the results (including publication)." Research facilities are encouraged to adopt a communication plan on what information (e.g., research data, experimental protocols) will be shared, including content to communicate, target audience, and communication method. The Dual-Use Guideline is "intended to assist regulated facilities in meeting the requirements specified in the CBS." Research facilities can choose alternate approaches to developing communication plans and managing communication risks (PHAC, 2018a).

PHAC's Dual-Use Guideline highlights the role of editors and editorial codes of conduct in limiting the publication of DURC, but this role remains contested (PHAC, 2018a). While editors can provide feedback on potential DURC implications of research papers, they may lack the required expertise and training to do so (NASEM, 2017).

The U.S. government has established stricter oversight of the communication of federally funded research on pathogens and toxins with dual-use potential (Gov. of United States, 2024b). The Implementation Guidance for the United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential ("the Implementation Guidance") provides that research institutions must develop a conduct and communication of research plan that is approved by the funding agency. Researchers bear the primary responsibility for ensuring that all communications, including research publications, adhere to the approved plan (Gov. of United States, 2024b). In the panel's experience, gain-of-function research papers often include biosafety and biosecurity practices in the materials and methods discussion as a safety measure.

### 4.3.3 Pre-publication review of research findings by Indigenous communities

To support data sovereignty, Indigenous data and knowledge systems require special consideration during the publication stage of the research process. The Global Indigenous Data Alliance notes that "the emphasis on greater data-sharing alone creates a tension for Indigenous Peoples who are also asserting greater control over the application and use of Indigenous data and Indigenous knowledge for collective benefit" (GIDA, n.d.). Indigenous and non-Indigenous people may have different perspectives on privacy and confidentiality, which are integral to data sovereignty (CCA, 2023a). For example, A First Nations Guide to the Privacy Act developed by the FNIGC provides that much of the First Nations data held by the Crown are not considered personal information under the *Privacy Act* and do "not recognize or accommodate First Nations collective rights to privacy … [and deny] most First Nations similar respect it gives to other governments, including foreign governments, provinces, and municipalities" (FNIGC, 2024). Indigenous communities' understanding of privacy can extend beyond data about people and include other knowledges (e.g., hunting and gathering practices, ceremonies) (Snipp, 2016). Communicating and reporting of research results to Indigenous communities often rely on methods similar to research monitoring (Section 4.2.4), as both phases of the research process are closely interconnected and should be guided by community priorities and values.

## 4.4 Safeguarding the research lifecycle

In Canada, researchers, institutions, governments, and Indigenous Peoples have implemented measures to safeguard sensitive research of concern. In practice, there is more safeguarding in pathogen research due to the high risk of negative impacts on human health through inadvertent or nefarious activities compared to ocean research. For all sensitive research of concern, it is important to re-assess and, if necessary, modify these measures throughout the research process to ensure a proper balance between security and research openness. Although it is often assumed that researchers—as subject matter experts and recipients of research funding—should bear the primary responsibility for safeguarding sensitive research of concern, successful implementation of these measures relies on shared

> Successful implementation of safeguarding measures relies on shared accountability across all actors in the research ecosystem

accountability across all actors in the research ecosystem—researchers, institutions, governments, and Indigenous Peoples.

The distribution of accountability across the research ecosystem may vary depending on the phase of the research process, the types of research, the source of research funding, and whether the research project involves Indigenous Peoples and their Land. The following considerations can help all actors of the research ecosystem assess whose participation is required to ensure the effective implementation of measures to safeguard sensitive research of concern:

- **Expertise**: The effective implementation of safeguarding measures depends on subject matter expertise in the relevant research field, alongside specialized knowledge of research security and open science principles. Examples of measures: self-imposed restrictions on publication and data-sharing; external pre-publication review of research findings.
- **Capacity and resources**: Actors with access to infrastructure, resources (e.g., staff, tools, training programs), and communities of practice are often best equipped to support the implementation of research security measures. Examples of measures: controlled access to research facilities, cybersecurity, travel policies.
- **Legal commitments:** Laws, regulations, contractual obligations, and funding agreements can assign the responsibility and accountability for the implementation of safeguarding measures to specific actors. Examples of measures: screenings of researchers and research proposals, bans on partnerships and collaborations, and security provisions of research agreements.
- **Indigenous rights and data sovereignty**: Indigenous Peoples should guide the development and implementation of all measures to safeguard sensitive research of concern that takes place in their communities and on their Land.

Key to this success is allocating resources and enabling decision-making systems that support researchers and institutions in these efforts. These same enabling factors should extend to Indigenous communities to uphold the right of Indigenous Peoples to determine what constitutes sensitive research of concern in their communities and how to safeguard it.

Measures to safeguard sensitive research of concern vary in scope and complexity but encounter similar obstacles due to the fragmented nature of the research security landscape, the inequitable distribution of responsibilities for safeguarding sensitive research, lack of capacity, and the chilling effects of

research security on research collaborations and open research. Chapter 5 discusses factors that can address these challenges to enable a research system that is as open as possible and as secure as necessary.

5

# Enabling Research Security While Balancing Open Science

## Chapter findings

- Factors that support research security measures may also apply to open science; determining the level of openness and security for research relies on the same foundation of enabling conditions, including financial resources.
- Enabling researchers to successfully engage with both open science and research security requires education, training, and capacity-building at individual and institutional levels.
- Divergent research security approaches across Canada and other jurisdictions cause confusion and reduce buy-in among researchers. Harmonizing support systems for knowledge-sharing across the research ecosystem and devoting resources to measuring and evaluating the outcomes of research security measures can improve effectiveness.
- Establishing widespread sensitivity to research security issues requires changes to research culture; the *modern research mindset* encompasses awareness of risks alongside research integrity and the responsible conduct of research.

The impact and ultimate success of measures for identifying and safeguarding sensitive research (Chapters 3 and 4) rely in part on enabling factors. Currently, supports for the implementation of these measures are inconsistent and lacking in certain sectors, and various actors within the research system are differentially impacted. Academic, government, and private industry actors are subject to different incentives and capacities when faced with the prospect of adopting new research security or open science practices, especially in fields where these practices are novel and experiences are limited. In several cases, the same supports apply to research security and open science; determining the level of openness and security for research relies on the same foundation of enabling conditions. Support systems for knowledge-sharing (Section 5.1), capacity-building and training (Section 5.2), financial resourcing (Section 5.3), and enforcement of compliance (Section 5.4) are all necessary to identify and safeguard sensitive research, while also potentially supporting open science and innovation.

## 5.1 Support systems for knowledge-sharing

Within Canada, jurisdictional approaches to research security differ, complicating inter-institutional partnerships and consistent implementation of research security policies across the country (UCalgary & U of A, 2023; SRO, 2024a). This variation impacts public funding because some funders align their research security efforts with federal programs (e.g., using the STRAC and NSGRP policies as guidance) while imposing additional requirements (Mitacs, 2023; Gov. of ON, 2024a); federal agencies and departments also have their own research security policies (e.g., NRC, 2024). In the panel's experience, this lack of harmonization imposes additional burdens on researchers, slowing down collaborative research among Canadian institutions and reducing buy-in for the implementation of research security measures. This issue is not limited to collaboration within Canada; differing approaches to research security across allied jurisdictions may reduce the effectiveness of global efforts and pose a challenge to researchers attempting to navigate international collaborations responsibly and securely. At the international level, The Five Eyes partnership and the G7 have introduced research security guidelines and policies addressed to academic researchers, governments, and the private sector in order to harmonize approaches across member states (SIGRE, 2022; CSIS, 2024a,c). The panel emphasizes that harmonization does not imply standardization. Utilizing common baseline criteria—including foundational principles and approaches to addressing challenges while maintaining unique processes tailored to specific circumstances—would be one way to reduce repetition and the burden on researchers and institutions responsible for implementing research security and open science policies.

Within Canada, jurisdictional approaches to research security differ, complicating inter-institutional partnerships and consistent implementation of research security policies across the country

Given the fragmented nature of mechanisms to identify and safeguard sensitive research, establishing support organizations tasked with the gathering and sharing of information on existing approaches is instrumental to

Differing approaches to research security across allied jurisdictions may reduce the effectiveness of global efforts and pose a challenge to researchers attempting to navigate international collaborations responsibly and securely

cultivating consistency across the research ecosystem, both within Canada and across foreign jurisdictions. Some strategies that may address this fragmentation are specialized centres that provide research advice, national roundtables and advisory groups, and the measurement and evaluation of research security activities.

### Specialized centres can provide tailored advice on research security and coordinate efforts within jurisdictions

While research security in Canada is distributed among different departments and agencies (Section 2.4), the Netherlands has adopted a whole-of-government approach and created an inter-ministerial National Contact Point for Knowledge Security to assist knowledge institutions and their affiliates with assessing risks and opportunities associated with international cooperation (OCW, n.d.-a). This service helps steer institutions and researchers towards publications and tools produced by government agencies and other trusted third parties, such as state actor threat assessments (e.g., AIVD *et al.*, 2022; OCW, 2023), advice on how to weigh security needs versus core principles of academic freedom and integrity (AWTI, 2022), and relevant codes of conduct that aim to supplement national guidelines (KNAW *et al.*, 2018; OCW, n.d.-b). This approach is similar to the Biosecurity Office that the Netherlands uses to oversee sensitive research of concern in the life sciences (RIVM, n.d.-a,-b). Likewise, the Government of Australia has appointed the National Counter Foreign Interference Coordinator to streamline efforts to stymie foreign interference across the government, as well as with non-government actors at higher risk, such as research institutions (UFIT, 2021; Gov. of Australia, 2025).

The Research Collaboration Advice Team (RCAT) in the United Kingdom is a cooperative initiative between government and academia created to provide institutions with official advice on research security in international partnerships (RCAT, n.d.). This initiative acts as an important conduit to aid the government in understanding how academics conceive of and manage risks, and considers how initiatives and practices can be improved (d'Hooghe & Lammertink, 2022). RCAT has been well received by the research community in the United Kingdom and lauded for fostering coordination among various actors and highlighting the importance of risk management and awareness (d'Hooghe & Lammertink, 2022; Department for Science, Innovation & Technology, 2023).

In 2024, the National Science Foundation (NSF) announced the formation of the SECURE Center led by the University of Washington and supported by nine institutions (NSF, 2024b). It was established to serve as an information clearinghouse, helping the research community identify and mitigate foreign

interference. It would share "information and reports on research security risks, provide training on research security to the science and engineering community and serve as a bridge between the research community and government funding agencies." It would also act as a hub for several regional centers managed by six universities nationwide. Experts from these institutions would "provide expertise on sensitive research, threat types, geopolitical analysis and international collaboration" while SECURE Analytics, led by Texas A&M University, plans to "provide enhanced expertise in the form of landscape analyses, risk modeling and data reporting through the SECURE Center." As it is not yet fully operational, the effectiveness of this centre cannot be assessed (NSF, 2024b).

Within Canada, the Research Security Centre, operated by PS, is tasked with a mandate similar to that of the SECURE Center, providing guidance and advice to the research community on how to safeguard their research (GC, 2024j). The Research Security Centre is composed of a network of six research security advisors distributed across Canada, with a central hub based in Ottawa (PS, 2024a). Each security advisor is responsible for providing advice to the institutions in their region, though the panel notes that regions are geographically broad, resulting in many institutions per advisor. This approach can be particularly effective in situations where advice is provided within a specific timeframe; for example, the National Contact Point for Knowledge Security in the Netherlands aims to provide service within 48 hours (OCW, n.d.-a,-c).

CSIS is also advancing research security by offering publicly available resources and engaging directly with university research communities through the Academic Outreach and Stakeholder Engagement (AOSE) program and with private sector investors through the Secure Innovation initiative (CSIS, 2024a,d). AOSE organizes roundtable events and workshops, attends conferences, and produces commissioned papers to engage with various sectors implicated in research security (CSIS, 2024b, 2025). However, panel members note that only limited information can be shared by CSIS through these resources due to security clearance considerations, and whatever information is available does not always reach researchers in both academia and industry.

Moreover, the panel acknowledges that when information about research security threats is shared with the public, it can be exploited by malicious actors to cause harm, and that these risks need to be carefully balanced against the benefits of keeping the research ecosystem informed about potential threats. Information-sharing by CSIS may be improved in the future through legislative amendments introduced to the *CSIS Act* through Bill C-70 to allow for "the disclosure of information, subject to privacy protections, to individuals

and organizations outside the Government of Canada, to help them build resiliency to threats to the security of Canada" (PS, 2024d). In the panel's opinion, ongoing improvements in communication channels among the intelligence community, researchers, and institutional administrations could raise researchers' awareness and incentivize them to integrate research security into their daily activities.

### Research security communities of practice have been created to bridge various sectors and share knowledge

In 2020, the Government of the United States established the National Science, Technology and Security Roundtable as a forum for actors from government, academic, and industry sectors to share knowledge on research security (NASEM, 2024). The 2024 capstone event, which concluded the roundtable's four-year term, "examin[ed] effective approaches to communicating threats and risks; [and] … shar[ed] best practices for addressing and mitigating threats and risks" (NASEM, 2024). Though this roundtable is now completed, participants at the capstone event noted that "it will be important to have a forum where academia, the private sector, federal research funding agencies, intelligence agencies, and law enforcement would be able to continue to come together for ongoing discussions to share information on research security threats and risks" (NASEM, 2025). In the United Kingdom, the Engineering Biology Responsible Innovation Advisory Panel (RIAP) is offering advice to the government on emerging risks to innovation in engineering biology, and is comprised of both academic and industry leaders (Gov. of United Kingdom, n.d.). RIAP maintains permanent communication between the government, industry, and academic sectors, enabling policy development and engagement across sectors on emerging risks (Gov. of United Kingdom, n.d.). In Japan, a consortium on research security and integrity within the university system has also been proposed to support activities addressing research security and integrity concerns, topics of increased interest in the country (Gov. of Japan, 2023; University of Tokyo, n.d.).

Communities of practice have also emerged in other venues. In Canada, research security directors across several academic institutions have created the Team Canada initiative to bring practitioners together to share resources, discuss best practices, and develop strategies to meet the needs of institutions across the country (Universities Canada, 2024). This is further expanded upon through regional communities of practice (e.g., the Alberta Research Security Community of Practice; UCalgary, 2025).

### The private sector is a major contributor to research in Canada and requires dedicated guidance to support research security efforts

While these types of forums can help develop promising practices, the needs and capacities of the private sector differ from those of universities and other research institutions (EC, 2024a). In Canada, the private sector is an important component of the research ecosystem (Section 2.1); it funds the most R&D, spending $32.9 billion in 2024 compared with the $18.5 billion spent by the higher education sector (StatCan, 2024a). Some jurisdictions, including Canada, have been boosting research security engagement with the private sector. CSIS provides briefings on research security to private sector companies conducting biopharmaceutical, life sciences, and data science research (PS, 2024e). Furthermore, security guidance and education are offered to emerging technology investors—specifically small- and medium-sized companies—to help them identify threats and assets that may be at risk, secure supply chains, and manage collaboration and international expansion risks (CSIS, 2024a).

Other jurisdictions are also providing guidance to the private sector. In the United Kingdom, the National Protective Security Authority and the National Cyber Security Centre have focused their efforts on protecting emerging innovative tech startups and spinouts against IP theft. The Secure Innovation toolkit contains advice and resources tailored to small companies that may otherwise lack cybersecurity expertise and resources (NPSA, 2023). In the United States, the Center for Security and Emerging Technology[13] has recommended the creation of a specialized research security clearinghouse situated within the most active R&D centres (Flagg & Arnold, 2021). The goals of such an organization would be to share information and resources (including for training and decision support) with researchers in the private sector while coordinating with federal partners (Flagg & Arnold, 2021). It is unclear, however, whether this initiative will be implemented, or if it is to be encompassed within the activities and mandate of the SECURE Center.

### Analysis of research security activities helps evaluate the effectiveness of measures

Efforts to measure and evaluate the effectiveness of research security strategies are nascent and challenged by a lack of

Efforts to measure and evaluate the effectiveness of research security strategies are nascent and challenged by a lack of evidence and clarity surrounding appropriate study methods and theoretical approaches

13 The Center for Security and Emerging Technology is a policy research organization within Georgetown University's Walsh School of Foreign Service.

evidence and clarity surrounding appropriate study methods and theoretical approaches (Dao *et al.*, 2024). This issue also extends to open science directives and policies. The Tri-Agency Research Data Management Policy mandates that all research institutions administering tri-agency funds must create an institutional research data management (RDM) strategy, and that all tri-agency grant proposals reflect best practices for RDM in their methodologies, and in some cases also submit a data management plan to the relevant agency (GC, 2021b). Similar to research security policies, policy non-compliance may breach the responsible conduct of research (GC, 2021b). The tri-agency does not, however, evaluate institutional strategies (GC, 2024c), nor is there evidence of monitoring or tracking on the implementation of this policy by the tri-agency (Tayler *et al.*, 2020).

Open science initiatives need to be monitored in order to better understand gaps and foster solutions (Cobey *et al.*, 2023); yet, there is limited understanding of the degree to which grant-holders in the Canadian research system abide by data management and open science policies more broadly (Tayler *et al.*, 2020). Without some form of auditing or benchmarking, it is difficult to track progress and to implement improvements to processes (Tayler *et al.*, 2020; Moher & Cobey, 2021; Alayche *et al.*, 2023). Even when research funded through the tri-agency is mandated to be made publicly available within 12 months of publication, in reality many researchers do not follow the Tri-Agency Open Access Policy on Publications (Larivière & Sugimoto, 2018; Paquet *et al.*, 2022). This finding extends to clinical trials as well, with registration and publication of clinical trial results (components of the open science ecosystem) in Canada lagging behind other countries (Alayche *et al.*, 2023). It appears that a lack of compliance with mandates does not result in significant consequences, and these consequences remain vague (Paquet *et al.*, 2022).

In the panel's view, these gaps in the measurement and tracking of the effectiveness of open science initiatives apply to research security measures as well. Some jurisdictions have launched dedicated research programs to address evidence gaps in the efficacy of research security policies. In 2023, the NSF announced the development of a new research on research security (RoRS) program to "more fully understand the nature, scope, challenges, and potential of research security across all research" (NSF, 2023). The NSF will fund research on a variety of topics including:

> *the nature and pervasiveness of research security threats; methods for identifying research security risks, and strategies for preventing and mitigating them; methods for strengthening research security protocol and approaches; the complex relationships between human behavior and research security policies; research security policies and their implications;*

> *research on organizational change around systemic and cultural factors as they pertain to research security; research on research security in the context of a particular field or discipline, especially in high-risk areas; [and] the international dimensions of research security.*
>
> (NSF, 2025)

In Germany, the Helmholtz Association, which includes 18 scientific research centres, launched a program entitled Further Development of Research Security in International Scientific Collaborations, which supports programs for enhanced research security across several institutes (Helmholtz, n.d.). The EU is putting in place initiatives to monitor the effectiveness of research security actions and establishing policy hubs (EC, 2024a,b). The European Commission monitors member progress on implementation of the 2024 Council of the European Union recommendation on research security based on established indicators and is asked to submit an implementation report every two years (EC, 2024a).

In the panel's view, streamlining and centralizing sources of research security information in Canada using specialized centres or advisory groups, could facilitate information-sharing across all actors of the research system. Harmonization of approaches could minimize the administrative burden on research institutions and researchers. Tracking and monitoring of approaches to research security and open science are necessary to evaluate the effectiveness of the various strategies and mechanisms discussed in this report, as well as to further develop an understanding of capacity-building and training needs.

## 5.2 Capacity-building and training

Adequate capacity is key to any measure for identifying or safeguarding sensitive research; funding, training, and infrastructure are all integral to ensuring actors in the research system are supported in research security and open science activities. In the panel's view, one objective of capacity-building and training could be the internalization of sensitivities to security issues. It is critical, however, that this be done while minimizing the burden on researchers.

### Capacity-building and implementation tools are essential supports for integrating research security policies into institutional cultures

Governments across many jurisdictions offer resources to researchers for identifying sensitive research. In certain cases, where identification responsibility is primarily held by researchers, the importance of effective

design and dissemination of such supporting information cannot be overemphasized. For example, the Government of Germany is not directly involved in identifying sensitive research or placing limitations on research partnerships due to the constitutionally protected right to freedom of research; however, federal ministries provide support and promote knowledge relevant to research security (Gov. of Germany, 1949; d'Hooghe & Lammertink, 2022). Although specialized research ethics committees (KEFs) exist to identify sensitive research (Section 3.2.2), the process occurs on an opt-in basis, and the German framework hinges on the capacity of the research community to acknowledge and understand the ethical landscape of its activities (Jakob *et al.*, 2024). To ensure that this self-regulatory capacity exists, detailed resources on due diligence, cybersecurity risks, recommended practices for collaboration, and training modules on establishing international partnerships and agreements are made available to German researchers (DLR, 2022, 2023, 2024; DAAD, n.d.). Similar online resources are provided by the Government of Canada to the research community (GC, 2021e,f; NSERC, 2024d), although there is no option to opt-in to a KEF-style review if a researcher is concerned.

Research institutions may also have some level of responsibility for providing training or capacity-building to researchers. For example, the United Kingdom has research security guidelines explicitly targeted at the governing bodies of universities, implicating them in a centralized contact point for researchers and the provision of adequate supports (d'Hooghe & Lammertink, 2022; Universities UK *et al.*, 2022). The Australian Research Council's (ARC) Countering Foreign Interference Framework details how universities holding ARC grants are responsible for training and educating staff on appropriate disclosure, and for the identification and reporting of potential risks (ARC, 2023). Many research institutions in Canada now have research security offices and officers that provide advice and outreach to researchers regarding best practices and requirements for safeguarding research (e.g., U of A, 2025; UVic, 2025; U of T, n.d.). These bodies can keep abreast of threats and developments in the risk landscape and develop tools and resources for researchers at their institutions (V. Gerdts, personal communication, 2025; P. Ferguson, personal communication, 2024). AI has also been used to help research institutions manage the increasing number of research security requirements in certain jurisdictions; for example, Rice University utilizes an AI tool called PRISM to accelerate the assessment of research security risks (Franklin, 2025).

Capacity-building resources are, in some places, supplemented by central contact points for research security, to provide advice to researchers who feel ill-prepared to assess risks or manage vulnerabilities. For example, in the Netherlands, the Biosecurity Office at the National Institute for Public Health

and the Environment offers a questionnaire to help researchers determine if their research is dual use (RIVM, n.d.-a,-c). This same office acts as a national information centre for the government and organizations that work with high-risk biological material. Similarly in Canada, the RSC is a national contact point offering guidance and advice (PS, 2024a).

### Colleges and institutions conducting research with quick turnaround times have unique research security needs

College research is undertaken in response to community and industry needs, often in partnership with small- and medium-sized Canadian companies (Polytechnics Canada & BHER, n.d.). According to the Colleges and Institutes Canada (CICan) 2023–2024 Applied Research Survey, about 0.3% of college applied research partnerships were conducted with international partners[14] (CICan, personal communication, 2025). However, with growing economic and geopolitical uncertainty and the complexity of research relationships, new research security measures were deemed necessary to protect researchers, institutions, and funders from potential misappropriation or misuse of college driven innovations (CICan, personal communication, 2025). Colleges also specialize in short-term research projects with quick turnaround times (e.g., project completion in under 1 year) (CICan, 2023); thus, any research security requirements, such as risk assessments that involve long wait times for permission to move forward, could inhibit the ability of colleges to engage in this type of research.

Through a series of working group discussions and input from the college community, ISED heard that the greatest barrier to research security initiatives in the college sector is inadequate resourcing, as limited administrative capacity and budget would make implementing any new research security measures challenging (ISED, personal communication, 2025). College community representatives indicated to ISED that initiatives that are implemented would likely require consideration of how to minimize burden and time delays to be effective in the college context. As of April 30, 2025, a research security approach is being piloted at four institutions in Canada to determine the feasibility of the approach and resource requirements for the most promising path forward for the broader college sector (ISED, personal communication, 2025).

14 CICan defines international partners as any foreign-based or foreign-owned organizations. However, organizations with a branch or satellite office in Canada that have been active for at least one year are categorized as a Canadian partner.

### Safeguarding sensitive research involves training for all actors in the research system, at regular intervals, and through multiple modes of communication

Measures to safeguard sensitive research include organization-wide awareness-building efforts and communication strategies, training on research security and integrity, and transparency regarding conflicts of interest and commitment (MPG, 2017; PHAC, 2018a; DOD, 2023; OSTP, 2024; ASIO, n.d.). Australia's University Foreign Interference Taskforce recommends conducting regular general training for all researchers, staff, and students to address expectations of appropriate research conduct, how foreign interference can occur on campus, and how to report concerns of foreign interference, intimidation, and harassment within the university or with appropriate authorities (UFIT, 2021). General training can then be customized to address specific objectives and target intended groups (e.g., researchers, students, administrative support services). For example, assessing risks related to geography requires different considerations than assessing ethical risks, and may demand different resources and awareness-raising activities (e.g., U15 & Universities Canada, 2019b; KNAW, 2023). To be effective, it is advised that training and awareness campaigns take place regularly and use multiple channels, both online (e.g., email communication, learning modules) and in person (e.g., team discussions and meetings) (Gov. of Netherlands, 2022).

Training focused on specific requirements, including government policies that impose additional legal obligations on researchers, may also be required to ensure appropriate compliance (JASON, 2024). For example, the EU recommendation accompanying export regulations describes how these apply to academic research activities, including publications, presentations, software, and data (EC, 2021a). This document provides examples and conditions under which research items may require screening, while acknowledging the accompanying tensions with open access to research. It outlines conditions and circumstances under which certain research outputs may be exempt from export controls and describes the procedure for ensuring compliance, carrying out risk assessment, and navigating the export of items with dual-use potential that do not appear on related lists (EC, 2021a). Canadian institutions and researchers lack awareness of export controls and sanction regimes, and could benefit from similar guidance and training (UCalgary & U of A, 2023). The panel also notes that research security training and education are not exclusive to academic institutions, and that those participating in the research ecosystem from within governments should also receive this important knowledge.

One risk to widespread training on research security could be the over-sensitization of individuals to certain risk profiles (e.g., countries with

high-risk institutions), resulting in discrimination and barriers to participation in research activities for certain staff and students (Gov. of Netherlands, 2022). As discussed in Chapter 3, lists of research institutions prohibited from partnerships may disadvantage researchers from those countries, even if they are not associated with the institutions in question (Section 3.2.1). The effects of these policies are already being felt in Canada, where some researchers are erring on the side of caution when collaborating or taking on students, and simply avoiding individuals who may not make it through the visa process (P. Ferguson, personal communication, 2025). This issue has been taken to the extreme in certain contexts, such as the now defunct U.S. China Initiative, which, in the efforts to counter Chinese economic espionage, instead resulted in widespread racial profiling of academics and researchers (Prasso, 2021). Harassment of individuals from certain nations may also come from the nations themselves; there have been cases where China has pressured Chinese students working or studying in North American institutions to provide information to the Chinese government about their research (Molloy & Johnson, 2025).

To address issues around discrimination, research institutions in the Netherlands are encouraged to promote "the academic values of freedom, respect, and open academic discussion" in the risk awareness training of researchers and education in general (Gov. of Netherlands, 2022). Another approach to avoiding discrimination against individuals from certain countries has been used in France, where the government may restrict physical access to certain facilities for certain individuals based on risk assessments (Gov. of France, 2012; CNRS, 2024). In Canada, the development of the STRAC policy was guided by the principle of non-discrimination, harassment, and coercion, explicitly stating that it does not target any nationality (ISED, 2023f). Institutional level protocols may also be explicit in how to conduct due diligence research in accordance with ethical and legal requirements, while upholding the principles of equity, diversity, and inclusion (SRO, 2025).

## 5.3 Financial resourcing

In the panel's view, sustained financial resourcing for both open science and research security initiatives is critical. Asking researchers and their institutions to engage in and be responsible for determining the sensitivity of the research they produce—and how to safely share and protect it—is dependent on commensurate funding that extends beyond one-off or unstable sources.

### Controlling access to sensitive research requires financial resources, increasing the cost of doing research

Financial considerations are particularly relevant when research security policies impose additional physical and cybersecurity requirements for storing, transmitting, and processing sensitive data, as well as safeguarding equipment (JASON, 2024). Requirements for open science also involve additional digital infrastructure (Goodchild *et al.*, 2023). For organizations working with immense volumes of data (e.g., the Canadian Integrated Ocean Observing System, Ocean Networks Canada) the mandate of open data includes achieving FAIR (Findable, Accessible, Interoperable and Reusable) data and implementing TRUST (Transparency, Responsibility, User focus, Sustainability and Technology) principles (ONC, 2021a,b; CIOOS, n.d.-a,-c). Implementing these principles requires substantial resources to "support the production, sharing, and reuse of data over its lifecycle," especially if the research is considered sensitive (Goodchild *et al.*, 2023).

Research security policies enacted by the federal, provincial, and territorial governments increase the administrative burden placed on universities, highlighting the need for additional funding to support research security programs and offices. By demonstrating rigour in research security, however, institutions may position themselves as a trusted partner for sensitive research, creating opportunities for new collaborations and forms of funding (SRO, 2024b). At the federal level, post-secondary institutions that receive more than $2 million in research funding are eligible for research security funding, which is calculated as a percentage of their federal research funding (TIPS, 2022). As a result, large universities receive a significantly greater share of funding than small- and medium-sized universities, while most colleges and polytechnics do not receive any research security funding (TIPS, 2024). This is a gap in the current research security landscape, as colleges are participants in Canada's R&D ecosystem and often collaborate with the private sector, including foreign partners (CICan, 2023). In the panel's opinion, inequitable distribution of research security funding creates vulnerabilities in the Canadian post-secondary research ecosystem, since smaller universities, colleges, and polytechnics are often approached by foreign partners. Providing base funding to establish research security capacity across all research institutions could help fill gaps in the research security landscape and ensure that all institutions are adequately

> Inequitable distribution of research security funding creates vulnerabilities in the Canadian post-secondary research ecosystem

supported. Alternative, more equitable forms of funding already employed in other research funding programs (e.g., Canada Research Chairs special allocation funding, Research Support Fund allocation grant model) could also be applied to support research security efforts in smaller research institutions (GC, 2025k,l).

### Research security training can be required as a condition of federal research funding

In the United States, the NSPM–33 requires that organizations implement a research security program if they receive more than US$50 million per year in total federal research funding (NSTC, 2022). These programs must include research security and export control training for relevant personnel, which covers threat awareness and identification, preparation for research security incidents, review of foreign partnerships, and compliance with export control processes and protocols. Incorporating these considerations into existing training efforts for the responsible and ethical conduct of research is suggested (NSTC, 2022). In the panel's view, these initiatives tie into the concept of a modern researcher, where awareness and sensitivity to research security and open science are integrated into education and training (Section 5.5).

### Resources that overcome barriers to information-sharing support both open science and research security

Resources, training, and supports for safeguarding and sharing research are required for all types of research, regardless of where they sit on the continuum of sensitivity. Adopting open science practices requires overcoming several barriers (Gownaris *et al.*, 2022; ISED, 2024c). Digital research infrastructure deficits are particularly salient to the Canadian context (Northrup *et al.*, 2022; The Alliance, 2024). Resourcing for RDM storage capacity is not keeping pace with the rate at which data are being collated, nor with the growing range of needs corresponding to given research domains (including specific requirements for safeguarding sensitive research) (The Alliance, 2021; Goodchild *et al.*, 2023).

Open-access publishing can demand significant financial resources (Owens, 2023b). Publications in open-access journals require article-processing fees that typically come out of research grants. If researchers do not publish in an open-access journal, they must locate and publish in a suitable repository, potentially following an embargo period (Owens, 2023b). A survey revealed that the issues of cost and access to repositories are key barriers, alongside concerns surrounding the lack of professional incentive for open-access publishing in Canada and the lack of enforcement of existing policies (ISED, 2024c). Although

the diamond open-access model is free for authors and readers, it still demands financial resources from funders, governments, or donations to operate (Zheng, 2021; Bilodeau, 2024). Funding for long-term storage and access is also lacking across all research disciplines, alongside dedicated funds for professional support staff (The Alliance, 2021).

Another challenge is providing access to appropriately formatted data in repositories or elsewhere, requiring expertise and changes to common workflows—which can be burdensome in the absence of rewards. In the panel's experience, this gap leads to inequities in how certain individuals and institutions are able to safeguard or provide access to knowledge and data. This is especially true for Indigenous governments, communities, and researchers (Box 5.1).

## Box 5.1 Supports for Indigenous data governance

Although this report has highlighted scenarios where Indigenous rights-holders are engaging in data sovereignty and governance efforts (Sections 3.2, 4.1–4.3), these efforts are not without costs. Creating data management plans and governance arrangements, purchasing and maintaining infrastructure, and building capacity in individuals tasked with these responsibilities all require adequate resourcing (CCA, 2023a). Several organizations have developed or are actively developing data governance strategies and plans, including the First Nations Information Governance Centre (FNIGC), Inuit Tapiriit Kanatami (ITK), and the Métis National Council (MNC) (ITK, 2018; FNIGC, 2020; Gabel & Henry, 2024). Sustained funding to achieve data governance goals and outcomes is paramount; "multi-year (predictable) and flexible funding instruments will be essential to support cost-effective planning, as well as to allocate and account for the funds based on priorities and needs. Predictability of funding will be key to attracting, developing, and retaining talents and skills" (FNIGC, 2020). The panel emphasizes, however, that costs are not the only barrier to Indigenous data sovereignty efforts; data aggregation, the lack of sharing research data back to communities, policies and legislation blocking Indigenous Peoples from accessing and using their own data, and the publication of results without permission from Indigenous individuals or organizations all persist throughout the research ecosystem (ITK, 2018; FNIGC, 2020).

## 5.4 Enforcement of compliance

There are a wide variety of approaches to the enforcement of research security activities among foreign jurisdictions; however, several countries employ approaches for safeguarding sensitive research that are based on self-regulation within the research sector (d'Hooghe & Lammertink, 2022). This affords flexibility to researchers and aims to reduce burdens relating to establishing external oversight. In Germany, this approach is most pronounced, where researchers and institutions collectively carry the responsibility for safeguarding sensitive research, pursuant to relevant laws (Leopoldina & DFG, 2022b). In contrast, the approach used in France is top-down and places responsibility for the protection of knowledge resources with the General Secretariat for Defence and National Security (SGDSN), an inter-ministerial body also responsible for the implementation and development of security and defence policies (d'Hooghe & Lammertink, 2022; SGDSN, n.d.). The degree to which authority is assigned to researchers dictates which levers may be available for compliance and enforcement measures.

Among the compliance measures currently in force, several rely on presenting researchers with disincentives. For jurisdictions where researchers rely heavily on competitive funding, restrictions on access to funding or funding programs can apply strong pressure towards compliance. This approach can be implemented in different ways: under the STRAC policy in Canada, access to federal funding can be curtailed for researchers based on the topic and the affiliations of participants in their proposed project (ISED, 2023f), whereas the Australian government has placed conditions on access to grant funding based on the demonstration of adequate research security risk management planning (ARC, 2023). The STRAC policy is within the scope of the Tri-Agency Framework: Responsible Conduct of Research, and any failure to comply with STRAC invokes allegations of breach of agency policies, and the institution hosting the researcher is responsible for conducting an inquiry and investigation if necessary (NSERC, 2025). The panel notes, however, that institutions' internal investigations of breach may not be as extensive as they should be because of concerns related to preserving reputation (e.g., Molloy & Johnson, 2025), and that outside of research funded through the tri-agency, there are no specific enforcement mechanisms to comply with research security practices.

The Secretariat on Responsible Conduct of Research (SRCR) is mandated to provide support for the Tri-Agency Framework: Responsible Conduct of Research, by "reviewing institutional investigation reports to ensure the process followed by the institution is in accordance with its own responsible

conduct of research policy and is consistent with the Framework," and "learn[ing] from and respond[ing] to emerging issues in research ethics and responsible conduct of research, in a national and international context" (GC, 2024k). In the panel's view, the SRCR may have opportunities to further support institutions and researchers in research security activities, despite not currently having any current role in the enforcement of policies.

Other measures used to incentivize compliance may involve the reduction of additional administrative burdens, legal penalties, and emphasis on reputational risks. In France, digital research security measures require that data stored within regulated institutions be labelled to indicate their sensitivity, as part of a broader DMP. The absence of such a plan, or the presence of unlabelled data, results in all data contained in that facility being considered sensitive by default, thereby preventing researchers from sharing their research results (SGDSN, 2018). Penalties for activities contravening research security policies may also be utilized. For example, in Canada, non-compliance with the conditions of a license for research on human pathogens and toxins from PHAC may result in administrative enforcement actions (e.g., suspension or revocation of license and security clearance) or penal enforcement actions (e.g., investigation and prosecution) (PHAC, 2024a). Legal penalties vary across jurisdictions, ranging from fines to imprisonment, and their form and thresholds are defined through various pieces of legislation governing different dimensions of research security (e.g., Gov. of France, 1990, 2012; GC, 1992; Gov. of Australia, 2018; Gov. of United States, 2022b; Gov. of Netherlands, 2023; Gov. of South Korea, 2023). Damage to reputation or standing, with implications for obtaining funding and the attraction and retention of students and staff, is another negative outcome that can be communicated to institutions and researchers as a risk of not employing adequate or appropriate research security measures (Gov. of New Zealand, 2020; d'Hooghe & Lammertink, 2022; UNZ, 2022; NPSA & NCSC, 2024).

### Practices in support of compliance and enforcement of new research security policies benefit from sensitivity to research context and the needs of researchers

Compliance with laboratory safety policies has been shown to be improved through an understanding of disciplinary cultures, which requires the participation of engaged experts (Silbey, 2022). For example, biologists and chemists are each required to conform to strict laboratory safety practices, but notions of contamination and hazards differ between these fields (Silbey, 2022). These and other distinctions can inform the design and implementation of compliance measures. Accounting for differences across disciplines and specific

research contexts may provide other opportunities by exploring how security policies might be deployed in a manner that addresses an unmet need for researchers (Shankar & Drake, 2022).

Cybersecurity policies can introduce vulnerabilities as a result of researchers circumventing measures perceived to impede research or be disproportionately onerous. One approach to mitigate this issue is to filter cybersecurity measures through the lens of research workflows and specific use cases (based on disciplines), and taking into account existing IT infrastructure and services to avoid overly tedious conditions for researchers (Shankar & Drake, 2022). This method mimics the German approach to research security, wherein considerations are embedded within existing procedures for research integrity, reducing the burden on researchers while taking advantage of their familiarity with existing policies and approaches (d'Hooghe & Lammertink, 2022).

Although no single solution presents itself for effectively overcoming barriers to data-sharing, strategies such as tailoring data-sharing incentives to specific research contexts and disciplines (Musker & Smith, 2021), alongside the provision of resources (financial and human) and infrastructure (Woods & Pinfield, 2022) are promising. A narrow focus on individual researchers is insufficient, since culture changes in research communities may be more effective in improving uptake (Plomp *et al.*, 2019; Woods & Pinfield, 2022). Internationally, some institutions have created specific roles within research departments and units; these are tasked with establishing discipline-specific data management support (Plomp *et al.*, 2019; TU Delft, n.d.; University of Cambridge, n.d.).

### Protections for whistleblowers can facilitate the disclosure of information to law enforcement agencies

In some jurisdictions, cooperation with law enforcement and national security agencies is central to research security policies and guidelines (UFIT, 2021; NSTC, 2022; ARC, 2023). Such interactions are necessary to keep researchers up-to-date on the scale and scope of problems posed by foreign influence (JASON, 2024). Whistleblower policies can enable researchers and staff members to report illegal or unethical practices with confidence (Gov. of Netherlands, 2022). The Government of Quebec, for example, adopted special protections for whistleblowers that facilitate the disclosure of wrongdoings committed or about to be committed against public bodies, including universities. The *Act to facilitate the disclosure of wrongdoings relating to public bodies* prohibits public bodies from taking reprisals against people who raise a complaint in good faith, and establishes a presumption that any disciplinary measure or activity that affects a person's employment is a reprisal (Gov. of QC, 2024a,b). In

situations where aspects of research security are enforced by law, such protections for whistleblowers can support researchers who try to employ the law but are discouraged or prevented from doing so by their institutions.

### Establishing widespread sensitivity to security issues will require changes to research culture

Creating a research culture that is aware of potential security risks may aid in the self-regulation of research security and open science. Although a full review and analysis of the topic is out of scope of this report, change management approaches offer a potential pathway for achieving some of these goals, though it is not without challenges. For example, individual achievement and self-reliance are valued in academia, which can make the culture resistant to change as a result of several contributing factors, including concerns around loss of time, lack of resources and support to implement change, complexity or uncertainty of the proposed change, and perceptions that there is minimal value to proposed changes (Lane, 2007). Beyond cultural resistance to change, the panel also notes that the current system of research incentives and focus on maximizing publication outputs may deter researchers from engaging in responsible research, with regard to both research security and open science considerations. The panel further notes, however, that the signing of the San Francisco Declaration on Research Assessment (DORA) by the tri-agency (NSERC, 2023) may be a potential first step in addressing this challenge in the future, as DORA emphasizes the "need to improve the ways in which the output of scientific research is evaluated" (DORA, 2012).

Another potential challenge is the shift in sentiments around collaborations with certain countries. Over the past several decades, Canada has had a strong relationship with China in the innovation and education sectors, with dedicated programs to increase partnership and knowledge exchange (GC, 2008; Davidson, 2017; Evans, 2022). Recent focus on limiting collaboration and affiliation with certain institutions, including those located in China (e.g. ISED, 2023e), is a reversal of course. In the panel's view, researchers who were previously encouraged to foster relationships with Chinese colleagues and institutions may require additional support to adapt to changing policies.

When change involves new regulatory oversight, inadequate communications regarding the scope and nature of regulation can create confusion, particularly when regulations governing an entire research ecosystem are interpreted in heterogeneous ways across institutions (Babb, 2020). For example, during the early 2000s, heightened enforcement of the Common Rule—a U.S. federal policy to protect human research subjects enacted in 1991 (Gov. of United States, 1991)—resulted in widespread dissatisfaction among researchers (Babb, 2020).

This stemmed from a lack of clarity on how to achieve compliance (ostensibly designed to provide flexibility to institutions) in combination with non-compliance penalties. Efforts to raise compliance were marked by a focus on the total elimination of risk, but they also led to confusion and frustration among researchers in fields that would typically be exempt from the Common Rule (particularly social sciences and humanities research) (Babb, 2020). Although research security is an issue separate from the ethical considerations outlined in the Common Rule, this example illustrates some of the implementation risks associated with a wide-ranging regulation of research, as well as challenges in defining compliance levels that reduce risk to a suitable level without negatively impacting research.

Understanding the culture of the environment where change is being pursued is essential to organizing implementation and communications planning (Berns *et al.*, 2007). In the setting of a public research institution, the creation of a dedicated body for supporting change management is important because it provides a central resource for individual research departments. Moreover, effective and clear communications and training of leadership are essential to implementation, since changes (and their consequences) may catch employees off guard (Berns *et al.*, 2007). In the case of research security, dedicated institutional bodies such as research security offices are tasked with raising risk awareness among faculty and staff, but the panel notes that these bodies may not have expertise in how to best institute change. Due to this lack of expertise, these offices may struggle to be effective in institutions with decentralized organizational structures. Incorporating change management expertise within research integrity or security offices and considering those principles in the development and implementation of research security policies may aid general uptake.

## 5.5 Fostering the modern research mindset

The implementation of measures to identify and safeguard sensitive research can be supported by enabling factors that are applicable across both research security and open science activities. Key to the success of these efforts is the creation of systems of shared accountability, where the responsibility for executing measures is distributed among actors who are best equipped to perform the relevant roles. This framing relates to the concept of the modern research mindset, in which all actors participating in the research ecosystem are aware of not only research security and their role in it, but also open science, ethics, and research integrity more broadly, allowing individuals to assess how open and secure their research needs to be. Quickly changing

geopolitical contexts and the rapid pace of technological advancement in research all contribute to the need for researchers to have a modern mindset capable of adaptation, and to be equipped with the tools and resources necessary to embody the following aspects:

- Participation in the protection and preservation of the Canadian research ecosystem, encompassing research security and open science, as well as innovation;
- Awareness of the global context in which research takes place, and how it may affect the responsible conduct of research;
- Application of an ethical, privacy, and security lens to research, especially in partnerships and collaborations (including with Indigenous Peoples and foreign partners);
- Prioritization of research integrity in all aspects of conducting and supporting research, throughout the lifecycle of a project; and
- Ongoing assessment of one's own research sensitivity in relation to changing geopolitical contexts.

The modern research mindset and the modern researcher are the outcomes of adequate training, resourcing, and capacity-building, all of which are necessary to support the development of vital competencies for participating in research in Canada looking to the future

In the panel's view, the modern research mindset and the modern researcher are the outcomes of adequate training, resourcing, and capacity–building, all of which are necessary to support the development of vital competencies for participating in research in Canada looking to the future.

6

# Conclusion and Final Reflections

Though various orders of government have instituted security policies to strengthen Canada's research ecosystem, rapid advancements in certain areas and the changing geopolitical landscape necessitate an ever-evolving approach to identifying and safeguarding sensitive research that balances research security and open science and innovation. Recognizing this, DRDC and PHAC asked the panel to examine measures to identify and safeguard sensitive research of concern, and how to apply these approaches to the two research areas:

- **Pathogen research** involves materials that pose great potential risk to human health and therefore features many stringent protocols and frameworks for the identification and safeguarding of research. This type of research is representative of other study areas where risks to human health and well-being are well known.
- **Ocean research** comprises a vast array of fields of study featuring varying sensitivities. Unlike in pathogen research, there is much less oversight and direction for researchers to gauge the sensitivity of their research, its potential negative impacts, and implement appropriate safeguards. Much of ocean research is focused on sharing information with a wide range of actors nationally and internationally, and researchers may not be considering research security measures to restrict access to this information.

Similar to ocean researchers, those conducting many other types of research, including in the social sciences, and humanities, may be unaware of the potential security risks associated with their research, even though their research outputs or methods may be sensitive due to privacy or ethical concerns.

Throughout the report, various means for identifying and safeguarding sensitive research and sensitive research of concern have been examined, including measures being used in Canada and approaches from other jurisdictions. Where possible, the applicability of these measures to pathogen or ocean research has been discussed. Section 6.1 summarizes these measures in the context of these two research areas, comparing and contrasting various approaches and discussing the factors required for implementation across the research design, active research, and post-research phases. Final reflections from the panel are shared in Section 6.2.

## 6.1 Application of measures to pathogen and ocean research

To make informed decisions about research security, those engaged in research activities need to know how to identify sensitive research and determine when it presents additional risks (i.e., becomes *of concern*). Balancing risks with opportunities in research is a critical component in the assessment of sensitivity and appropriate safeguards, where research that is extremely valuable to human health and global well-being (e.g., infectious disease research, geospatial data) is also often associated with security risks. Factors that trigger the identification of research as sensitive depend on the research area and project. Lists of sensitive technologies, risk assessments, and consultations with experts are common tools employed in the identification of sensitive research in Canada and other jurisdictions. Once research has been identified as sensitive and of concern, appropriate safeguards must be determined to ensure it is responsibly conducted and shared. The panel emphasizes that not all safeguards are appropriate to all types of sensitive research of concern; when they are applicable, implementation may differ.

The panel emphasizes that not all safeguards are appropriate to all types of sensitive research of concern; when they are applicable, implementation may differ

### 6.1.1 Identifying and safeguarding sensitive pathogen research of concern

In pathogen research, factors that signal sensitivity include risks to human health, harmful application of research, and context-specific factors such as the transmissibility of pathogens. When the risk of conducting research is evident, and the consequences of its potential misuse can be detrimental to public health and safety, policy-makers create lists of dangerous items and products and restrict who is allowed to conduct research. This is the case for research involving certain types of human toxins and pathogens. While a list-based approach is the main mechanism to identify sensitive research of concern related to pathogens, it is supplemented by additional measures—risk assessments and specialized expert reviews—designed to reinforce the application of lists (Table 6.1).

## Table 6.1 Measures to identify sensitive research of concern in pathogen research

| Measure | Description | Phase of research process |
|---|---|---|
| Lists | Research with pathogens and toxins included in the *Human Pathogens and Toxins Act* requires specific safeguarding measures, including licences and security clearance. These materials also appear on export control lists, which require an export licence or permit, in accordance with the Australia Group lists of chemical and biological weapons. | Research design phase; post-research phase |
| Risk assessments | The Canadian Biosafety Guideline provides a decision tree and risk assessment process to aid in determining the level of sensitivity of certain types of research. Considerations for novelty, harmfulness, modification risk, and misuse potential are all included in the risk assessment process. Once the risks are identified, a further step is taken to determine if the existing level of biosafety is adequate, or if additional safeguarding measures are required. | Research design phase |
| Specialized expertise | Certain journals screen submissions for dual-use potential and identify research that is too sensitive to be published in the proposed state, if at all. | Post-research phase |

Once work has been identified as sensitive and of concern in pathogen research, a host of safeguarding measures apply to the research design phase. In many cases, these measures are embedded in policies (e.g., the Canadian Biosafety Standard) adopted under the *Human Pathogens and Toxins Act (HPTA)* and the *Human Pathogens and Toxins Regulations (HPTR)*. The active research and post-research phases are less regulated. For example, with regard to cybersecurity, the Biosecurity Addendum to the Biosafety Standard, which enters into force in 2026, will apply only to containment level 4 research facilities. In the post-research phase, the development of communication plans is left to the discretion of licensed research facilities (Table 6.2).

### Table 6.2 Measures to safeguard sensitive research of concern in pathogen research

| Measure | Description | Phase of research process |
|---|---|---|
| Screening of researchers and partners | Researchers undertaking research with SSBAs must acquire special security clearance, while foreign nationals must provide additional documentation. | Research design |
| | Pathogen researchers applying for federal funding for projects that involve the application of life sciences technology (as identified in the STRAC policy) cannot collaborate with researchers affiliated with named research organizations (NROs). | Research design |
| Screening of research | Licences are required for research concerning pathogens and toxins identified as risk groups two, three, and four. | Research design |
| | Research facilities adhering to the Canadian Biosafety Standard are required to review all projects for dual-use potential at all stages, including in the dissemination of results. | Research design phase; active research phase; post-research phase |
| | PHAC recommends that research facilities adopt communication plans dictating what information can be shared and with whom. | Post-research phase |
| Security of research facilities and infrastructure | Controlled access to research facilities is a common practice in both public and private labs working with pathogens and toxins. | Active research phase |
| | Requirements for level 4 facilities that enter into force in 2026 will include a cybersecurity plan, policies on the use of digital devices, and a system for labelling, working with, and limiting access to sensitive information. | Active research phase |

## 6.1.2 Identifying and safeguarding sensitive ocean research of concern

Although the higher-level processes for identifying and safeguarding ocean and pathogen research are aligned, ocean research differs from pathogen research in that the sensitivity risks of conducting the former are often not as obvious, with less potential immediate harm to human health and well-being; some factors that can trigger research to be sensitive are foreign partnerships, research concerning Indigenous Peoples, geography, and the production and use of large datasets. Simultaneously, the sharing of large volumes of ocean observation data are foundational to international partnerships that advance understanding of climate change and other global issues. The sensitivity of research can depend on whether the researcher advances certain technologies included in the STRAC policy, works in sensitive research areas, or with certain

types of data. Risk assessment committees can be established to provide additional guidance to researchers and determine, whether research identified as sensitive presents additional risks (i.e., is of concern) because it can be reasonably anticipated to be misappropriated or misused immediately or in the future, with no or minimal modifications (Table 6.3).

### Table 6.3 Measures to identify sensitive ocean research of concern

| Measure | Description | Phase of research process |
|---|---|---|
| Lists | Ocean research that advances certain technologies is implicated in the STRAC policy. These technologies (under the category of advanced sensing and surveillance) appear on the list of sensitive technologies that, on their own, do not indicate the research is of concern but can be cross-referenced with the NRO list. Institutions may assess their strengths through prized asset analysis, and create and periodically re-assess lists of sensitive research areas (which could include ocean research) that warrant additional safeguards. | Research design phase; active research phase |
| Risk assessments | Standardized risk assessments are not commonly used in ocean research, partially due to the lack of familiarity of individual researchers with respect to research security. Institutional review boards could be tasked with performing risk assessments of particular research areas in conjunction with researchers. These bodies can be internal to institutions, regional, or rely on national research organizations such as the Oceans Research in Canada Alliance (ORCA) to coordinate and provide services to the ocean research community. | Research design phase; active research phase |
| Specialized expertise | Certain types of ocean monitoring data (such as acoustics) are extremely valuable to national and international scientific goals but also have military implications. Specialized screening and expertise within the military is necessary to prevent certain data from inclusion in publicly accessible dataflows for national security reasons. Indigenous research partners also hold specialized expertise in identifying data or research that may be culturally sensitive, dictating the conditions of sharing and access. | Research design phase; active research phase; post-research phase |

Most measures to safeguard ocean research of concern apply on a case-by-case basis, depending on the applicable policies of research institutions and researchers' awareness of security risks. Policies promulgated by the federal government, such as NSGRP and STRAC, can provide helpful guidance in this regard. Some safeguarding measures may be attached to private and public

funding (e.g., a risk assessment process under the NSGRP or limitations on publishing research results) (Table 6.4).

### Table 6.4 Measures to safeguard sensitive research of concern in ocean research

| Measure | Description | Phase of research process |
|---|---|---|
| Screening of researchers and partners | Foreign ocean researchers applying to work and study in Canada are subject to security screenings by government agencies. | Research design |
| | Ocean researchers and organizations can rely on the NRO list to avoid collaborations with researchers affiliated with foreign entities that pose security risks. | Research design |
| Screening of research | An ocean researcher applying for tri-agency funding must submit a risk assessment form with their grant application if their funding opportunity falls under the NSGRP and they plan on conducting research with a qualifying partner. | Research design |
| | Organizations that fund ocean research may use the NSGRP to guide the security review of research proposals based on open-access sources. | Research design |
| | Data-labelling systems controlled by Indigenous Peoples can support continuous monitoring of the active research phase in compliance with the principle of data sovereignty. | Research design phase; active research phase; post-research phase |
| Restrictions on publications and sharing | Restrictions on the publication and sharing of data may be imposed on a case-by-case basis (e.g., through research contracts or by the principle of data sovereignty). | Post-research phase |
| Security of research facilities and infrastructure | Ocean research organizations can implement cybersecurity and data management policies. | Active research phase |

## 6.1.3 Comparing and contrasting approaches

Measures for identifying and safeguarding sensitive research of concern may be broadly applied across many areas of research, though the precise method of implementation may vary. No single measure is appropriate for all types of research, nor should it be as the risk landscape is unique for each research area, and each individual research project. Determining the level of risk for each unique research project, and implementation of appropriate actions and safeguards, is critical to avoid the oversecuritization of research and

researchers, and to ensure that research and data continue to be shared to advance knowledge and innovation. In this report, pathogen and ocean research can be viewed as stand-ins for other research areas with varying levels of regulation and awareness of risks by researchers and their institutions. For example, nuclear research shares some similarities to pathogen research in that it is highly regulated and protected, with broad general knowledge of the potential harms to humans. Ocean research can be analogous to many other areas of the research ecosystem where emphasis on research security is limited. The panel emphasizes that this assessment does not provide a comprehensive description of all potential measures for identification and safeguarding, however those listed are a starting point for researchers and institutions to determine which may be most applicable to address the risks of research areas in question. Other types of sensitivity triggers (Table 3.1) may emerge depending on the discipline or research area, and the approaches to identify and safeguard research may be applied individually or in tandem, in a variety of ways. No matter the measure, adequate policy, guidance, resources, and supports are critical for successful implementation.

> No single measure is appropriate for all types of research, nor should it be as the risk landscape is unique for each research area, and each individual research project

### 6.1.4 Conditions for success

Various efforts are underway to bolster research security in Canada and in foreign jurisdictions, but concerted efforts are needed to assess these measures, as well as their impacts on open science and innovation. Though limited, evidence indicates that measures require financial (and other) resources, capacity-building, training, and knowledge-sharing to enable and empower individuals, communities, and institutions undertaking the work of research security and open science (Chapter 5). Many of these considerations, although discrete and involving different objectives and actors, can fall under the umbrella of the responsible conduct of research. Ensuring that researchers, supported by their institutions and governments, are adequately trained in responsible conduct relies on the identification and protection of sensitive research, as well as an understanding of open science; this enables them to create research that is as open as possible and as secure as necessary.

## 6.2 Panel reflections

### There is a shared accountability for research security and open science in Canada

The responsible conduct of research is expected of all actors in the research system and involves a suite of measures that work in tandem. The panel understands that, building on the good work already being done in Canada to advance research security, there are opportunities to grow and improve. There is no single strategy or measure that can effectively identify or safeguard all sensitive research. Similarly, no single actor in the research ecosystem can be responsible for creating and implementing these measures. Working together to harmonize approaches to research security and open science within Canada will help reduce the burden on researchers and minimize confusion when they attempt to work across jurisdictions, both within Canada and internationally. The panel further suggests that there is a social responsibility and civic duty for all who engage in research to be accountable for the appropriate conduct of research, including but not limited to research security and openness. Much of the research done in Canada is publicly funded, and therefore researchers and other actors in the ecosystem should be encouraged to ensure their findings are not only of use and for the good of people in Canada, but also, if necessary, that people are protected from the possible misuse of research. In parallel, decision-makers have an important role in ensuring that guidance is clear and that adequate supports are available for researchers and institutions to fulfill research security and open science directives, while minimizing administrative burden and financial costs.

### A modern research mindset encompassing multiple competencies can support the responsible conduct of research

In the panel's view, the concepts of the modern research mindset and the modern researcher are promising for effecting change that supports both research security and open science. They refer to cultivating awareness of security and open science in researchers throughout their academic careers, as well as individuals comprising research institutions and governments more broadly. These skills could be introduced as a training requirement by institutions or departments, and supported by governments and decision-making bodies. Training could also be supported at the faculty level by making it a requirement for receiving federal research funds. This training would focus on the principle that engaging in the responsible conduct of research involves sensitivity to potential risks in tandem with engagement on open science and research integrity, to avoid oversecuritization. Researchers,

institutions, and funders must view security awareness and the value of open science as fundamental skills in the research ecosystem. In the panel's view, senior leaders are critical in this process; if they do not also develop and value these competencies, it will be much more difficult for institutional culture to change and adapt.

### Research security will likely become increasingly important in the future, and successful implementation of measures warrants expanded evaluation, monitoring, and tracking of initiatives

If threats to intellectual activities continue, there could be devastating consequences that are far-reaching across society, with negative impacts on health, wealth, and our ways of life. Because of these potential impacts, the panel sees this report as a tool to support a call to action for increased recognition of research security across the research ecosystem by all actors. These efforts need to be pan-Canadian in scope to be effective in an ever-changing geopolitical landscape, with approaches coordinated across allied and collaborative jurisdictions. Changing externalities warrant the continuous re-assessment of risks to enable a responsive and flexible approach to research security. Conversations and dialogue also need to continue between researchers and those active within national security and intelligence communities so that all are aware of the changing geopolitical context and are able to continually re-assess the sensitivity of research. The Arctic is a critical example of this; some areas of research are rapidly becoming more sensitive as the North becomes increasingly politicized.

Monitoring and tracking of compliance and effectiveness of these policies and programs is crucial to improving implementation and ensuring that all actors in the research system are adequately supported to make research as open as possible and as secure as necessary

Research security and open science initiatives—under the broader concept of responsible conduct of research and research integrity—are vital to the research ecosystem, and yet it is difficult to identify the most promising practices due to a lack of publicly available research and evaluation of current programs both in Canada and internationally. Monitoring and tracking of compliance and effectiveness of these policies and programs is crucial to improving implementation and ensuring that all actors in the research system are adequately supported to make research as open as possible and as secure as necessary. Canada's research ecosystem does not and will not ever exist in a

national vacuum; therefore, ongoing dialogue about approaches to identifying and securing sensitive research without compromising open science are necessary on an international stage. There is an opportunity for Canada to be a leader in these conversations, promoting both open science and the sharing of research where safe, and securing sensitive research of concern to ensure the safety and well-being of people in Canada and across the world.

# References


AIVD, MIVD, & NCTV (General Intelligence and Security Service, Military Intelligence and Security Service, and National Coordinator for Security and Counterterrorism). (2022). *Dreigingsbeeld Statelijke Actoren 2 [Threat Assessment of State Actors]*. Zoetermeer, the Netherlands: AIVD, MIVD & NCTV. https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

Akhtar, S. I. (2024). *USMCA: Intellectual Property Rights (IPR)*. Washington, D.C.: U.S. Congressional Research Service. https://www.congress.gov/crs_external_products/IF/PDF/IF11314/IF11314.6.pdf.

Alayche, M., Cobey, K. D., Ng, J. Y., Ardern, C. L., Khan, K. M., Chan, A.-W., … Moher, D. (2023). Evaluating prospective study registration and result reporting of trials conducted in Canada from 2009 to 2019. *FACETS*, *8*, 1–10. https://doi.org/10.1139/facets-2022-0208.

ARC (Australian Research Council). (2023). *ARC Countering Foreign Interference Framework*. Canberra, Australia: ARC. https://www.arc.gov.au/sites/default/files/2023-12/ARC%20Countering%20Foreign%20Interference%20Framework.pdf.

ARC (Australian Research Council). (n.d.). Research security. Retrieved August 2024, from https://www.arc.gov.au/funding-research/research-security.

Around Him, D., Aguilar, T. A., Frederick, A., Larsen, H., Seiber, M., & Angal, J. (2019). Tribal IRBs: A framework for understanding research oversight in American Indian and Alaska Native communities. *American Indian and Alaska Native Mental Health Research*, *26*(2), 71–95. https://doi.org/10.5820/aian.2602.2019.71.

ASIO (Australian Security Intelligence Organisation). (n.d.). *Protect your Research, Collaborate with Care*. Canberra, Australia: ASIO. https://www.asio.gov.au/system/files/2023-05/Protect%20Your%20Research%2C%20Collaborate%20with%20Care%20-%20Booklet.pdf.

ASM Journals (American Society for Microbiology). (2021). Dual use research. Retrieved June 2025, from https://journals.asm.org/dual-use-research.

Asselin, R. (2024). *Engines of Growth*. Ottawa, ON: Business Council of Canada. https://www.thebusinesscouncil.ca/wp-content/uploads/2024/08/Engines-of-Growth.pdf.

Asselin, R. & Speer, S. (2019). *A New North Star: Canadian Competitiveness in an Intangibles Economy*. Ottawa, ON: Public Policy Forum. https://ppforum.ca/wp-content/uploads/2019/04/PPF-NewNorthStar-EN4.pdf.

AWTI (Netherlands Advisory Council for Science, Technology and Innovation). (2022). *Knowledge in Conflict: Striking a Balance between Security and Liberty*. The Hague, the Netherlands: AWTI. https://www.awti.nl/documenten/adviezen/2022/11/29/advice-knowledge-in-conflict.

Babb, S. (2020). *Regulating Human Research: IRBs from Peer Review to Compliance Bureaucracy.* Stanford, CA: Stanford University Press.

BCC (Business Council of Canada). (2023). *Economic Security is National Security: The Case for an Integrated Canadian Strategy.* Ottawa, ON: BCC. https://www.thebusinesscouncil.ca/wp-content/uploads/2022/07/Economic-Security-is-National-Security-Report_digital.pdf.

BCC (Business Council of Canada). (n.d.). Our members. Retrieved June 2025, from https://www.thebusinesscouncil.ca/about-us/our-members/.

Belli, L., Gaspar, W. B., & Singh Jaswant, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, *54*, 106017. https://doi.org/10.1016/j.clsr.2024.106017.

Berns, K. A., Charboneau, D., Foth, C. J., Hesley, J., & Korsmo-Kennon, P. (2007). *Directing Change Management at the University of Minnesota.* Minneapolis, MN: University of Minnesota Twin Cities. https://conservancy.umn.edu/server/api/core/bitstreams/ec0e9e79-cd7a-45c8-a9e3-b2d3ad233542/content.

Bernstein, M. S., Levi, M., Magnus, D., Rajala, B., Satz, D., & Waeiss, C. (2021). ESR: Ethics and society review of artificial intelligence research. *arXiv. Preprint*. http://arxiv.org/abs/2106.11521.

Bilodeau, M. (2024, August 21). Open access: A diamond in the rough? *University Affairs*. Retrieved June 2025, from https://universityaffairs.ca/news/open-access-a-diamond-in-the-rough/.

BIS (Bureau of Industry and Security of the U.S. Department of Commerce). (2024). *Export Administration Regulations*, 15 CFR.

Brady, A.-M. (2017). *China as a Polar Great Power.* Cambridge, United Kingdom: Cambridge University Press.

Brandusescu, A. (2021). *Artificial Intelligence Policy and Funding in Canada: Public Investments, Private Interests*. Montréal, QC: Centre for Interdisciplinary Research on Montreal, McGill University. https://www.mcgill.ca/centre-montreal/files/centre-montreal/publicaipolicyandfunding_report_updated_mar5.pdf.

Brenneis, A. (2024). Assessing dual use risks in AI research: Necessity, challenges and mitigation strategies. *Research Ethics*, *21*(2), 302–330. https://doi.org/10.1177/17470161241267782.

Breum, M. (2024, January 23). The lack of data from Russia may render Arctic climate forecasting meaningless. *Arctic Today*. Retrieved November 2024, from https://www.arctictoday.com/the-lack-of-data-from-russia-may-render-arctic-climate-forecasting-meaningless/.

Brockmann, K., Bauer, S., & Boulanin, V. (2019). *BIO PLUS X: Arms Control and the Convergence of Biology and Emerging Technologies*. Solna, Sweden: Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2019-03/sipri2019_bioplusx_0.pdf.

CACN (Special Committee on the Canada–People's Republic of China Relationship). (2024). *The Nexus between Science and National Security in Canada: The Case of the National Microbiology Laboratory in Winnipeg*. Ottawa, ON: House of Commons. https://www.ourcommons.ca/Content/Committee/441/CACN/Reports/RP13349277/cacnrp08/cacnrp08-e.pdf.

Carroll, S. R., Herczog, E., Hudson, M., Russell, K., & Stall, S. (2021). Operationalizing the CARE and FAIR Principles for Indigenous data futures. *Scientific Data*, *8*, 108. https://doi.org/10.1038/s41597-021-00892-0.

Casadevall, A., Dermody, T. S., Imperiale, M. J., Sandri-Goldin, R. M., & Shenk, T. (2015). Dual-use research of concern (DURC) review at American Society for Microbiology journals. *mBio*, *6*(4), e01236-15. https://doi.org/10.1128/mBio.01236-15.

CBC News. (2014, August 13). Klaus Nielsen pleads guilty to trying to export infectious agent. *CBC News*. Retrieved June 2025, from https://www.cbc.ca/news/canada/ottawa/klaus-nielsen-pleads-guilty-to-trying-to-export-infectious-agent-1.2735012.

CBC News. (2024, April 12). Former Canadian Space Agency engineer acquitted on charge of acting for Chinese firm. *CBC News*. Retrieved July 2025, from https://www.cbc.ca/news/canada/montreal/space-agency-spying-quebec-1.7171861.

CCA (Council of Canadian Academies). (2013). *Ocean Science in Canada: Meeting the Challenge, Seizing the Opportunity*. Ottawa, ON: The Expert Panel on Canadian Ocean Science, CCA. https://doi.org/10.60870/me0n-6644.

CCA (Council of Canadian Academies). (2017). *Science Policy: Considerations for Subnational Governments*. Ottawa, ON: A Workshop Steering Committee Report, CCA. https://doi.org/10.60870/sen8-4y39.

CCA (Council of Canadian Academies). (2021). *Degrees of Success*. Ottawa, ON: The Expert Panel on the Labour Market Transition of PhD Graduates, CCA. https://doi.org/10.60870/fzwb-fg06.

CCA (Council of Canadian Academies). (2023a). *Northern Research Leadership and Equity*. Ottawa, ON: Expert Panel on the Future of Arctic and Northern Research in Canada, CCA. https://doi.org/10.60870/nna0-m891.

CCA (Council of Canadian Academies). (2023b). *Quantum Potential*. Ottawa, ON: Expert Panel on the Responsible Adoption of Quantum Technologies, CCA. https://doi.org/10.60870/bmzd-3e12.

CCA (Council of Canadian Academies). (2024a). *Navigating Collaborative Futures*. Ottawa, ON: Expert Panel on International Science, Technology, Innovation, and Knowledge Partnerships, CCA. https://doi.org/10.60870/gb8v-px63.

CCA (Council of Canadian Academies). (2024b). *Equity, Diversity, and Inclusion in the Post-Secondary Research System*. Ottawa, ON: Expert Panel on EDI Practices for Impactful Change, CCA. https://doi.org/10.60870/kx7v-vj32.

CCA (Council of Canadian Academies). (2025). *Research Security in Canada and Foreign Jurisdictions*. Ottawa, ON: CCA. https://cca-reports.ca/wp-content/uploads/2025/10/Balancing-Research-Security-and-Open-Science-EN.pdf.

CFI (Canada Foundation for Innovation). (n.d.-a). Major Science Initiatives Fund. Retrieved March 2025, from https://www.innovation.ca/apply-manage-awards/funding-opportunities/major-science-initiatives-fund.

CFI (Canada Foundation for Innovation). (n.d.-b). Research security. Retrieved February 2025, from https://www.innovation.ca/apply-manage-awards/resources-apply-manage-award/research-security.

Chase, S. (2022, August 9). Alberta relaxes some restrictions on university partnerships with links to Chinese government. *The Globe and Mail*. Retrieved January 2025, from https://www.theglobeandmail.com/politics/article-alberta-university-partnerships-chinese-government/.

CICan (Colleges & Institutes Canada). (2023). *Canadian Colleges: Creating IP and Powering Commercialization: Submission to the House of Commons Standing Committee on Science and Research – Study on the Commercialization of Intellectual Property.* Ottawa, ON: CICan. https://www.ourcommons.ca/Content/Committee/441/SRSR/Brief/BR12369907/br-external/CollegesandInstitutesCanada-e.pdf.

CIHR, NSERC, & SSHRC (Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council). (2022). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2).* Ottawa, ON: Government of Canada. https://ethics.gc.ca/eng/documents/tcps2-2022-en.pdf.

CIOOS (Canadian Integrated Ocean Observing System). (n.d.-a). About CIOOS. Retrieved November 2024, from https://cioos.ca/about/.

CIOOS (Canadian Integrated Ocean Observing System). (n.d.-b). Ocean data for our ocean future. Retrieved November 2024, from https://cioos.ca/.

CIOOS (Canadian Integrated Ocean Observing System). (n.d.-c). Data management resources. Retrieved February 2025, from https://cioos.ca/data-management-resources/.

CIRNAC (Crown-Indigenous Relations and Northern Affairs Canada). (2022a). *Inuit Nunangat Policy.* Ottawa, ON: Government of Canada. https://www.rcaanc-cirnac.gc.ca/eng/1650556354784/1650556491509.

CIRNAC (Crown-Indigenous Relations and Northern Affairs Canada). (2022b). Shipping in the Arctic. Retrieved June 2025, from https://www.cirnac.gc.ca/eng/1648145733596/1648145784817.

CLS (Canadian Light Source). (n.d.). Research security. Retrieved March 2025, from https://www.lightsource.ca/users/your-cls-experiment/practical-information/research-security.php.

CNRS (Centre national de la recherche scientifique). (2024). Call for evidence. Boosting research security in the EU. Contribution du Centre national de la recherche scientifique. Retrieved August 2024, from https://international.cnrs.fr/wp-content/uploads/2024/01/Contribution-du-CNRS-au-Call-for-Evidence-on-Research-Security-FR.pdf.

CNSC (Canadian Nuclear Safety Commission). (2014). FAQs: End-use controls. Retrieved February 2025, from https://www.cnsc-ccsn.gc.ca/eng/nuclear-substances/import-and-export-controls/index-faq/.

cOAlition S. (n.d.-a). Organisations endorsing Plan S and working jointly on its implementation. Retrieved September 2024, from https://www.coalition-s.org/organisations/.

cOAlition S. (n.d.-b). Plan S: Making full and immediate open access a reality. Retrieved June 2025, from https://www.coalition-s.org/.

CoARA (Coalition for Advancing Research Assessment). (2022). *Agreement on Reforming Research Assessment*. n.l.: CoARA. https://coara.eu/app/uploads/2022/09/2022_07_19_rra_agreement_final.pdf.

CoARA (Coalition for Advancing Research Assessment). (2025). Signatories. Retrieved June 2025, from https://coara.eu/agreement/signatories/.

Cobey, K. D., Haustein, S., Brehaut, J., Dirnagl, U., Franzen, D. L., Hemkens, L. G., … Moher, D. (2023). Community consensus on core open science practices to monitor in biomedicine. *PLOS Biology*, *21*(1), e3001949. https://doi.org/10.1371/journal.pbio.3001949.

COGR (Council on Governmental Relations). (2023). *Multi-Agency Panel on Research Security Risk Assessment & Analysis*. Washington, D.C.: COGR. https://www.cogr.edu/sites/default/files/Multi-Agency%20Research%20Security%20Panel_0.pdf.

COGR (Council on Governmental Relations). (2024). *Overview of OSTP Guidelines for Research Security Programs at Covered Institutions*. Washington, D.C.: COGR. https://www.cogr.edu/sites/default/files/Overview%20of%20OSTP%20Guidelines%20for%20Research%20Security%20Programs%20at%20Covered%20Institution%20clean%20copy%20july%2012%202024%20REVISED.pdf.

CoreTrustSeal Standards and Certification Board. (2022). CoreTrustSeal Requirements 2023–2025. *Zenodo. Preprint*. https://zenodo.org/record/7051011.

COS (Center for Open Science). (n.d.). What is open science? Retrieved August 2024, from https://www.cos.io/open-science.

CRCC (Canada Research Coordinating Committee). (2025). Program characteristics. Retrieved November 2024, from https://www.sshrc-crsh.gc.ca/funding-financement/nfrf-fnfr/characteristics-caracteristiques-eng.aspx.

CSIS (Canadian Security Intelligence Service). (2020). *Far From Home: A Travel Security Guide*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/far-from-home.html.

CSIS (Canadian Security Intelligence Service). (2024a). Secure innovation: Security advice for emerging technology investors. Retrieved February 2025, from https://www.canada.ca/en/security-intelligence-service/corporate/publications/secure-innovation-investors.html.

CSIS (Canadian Security Intelligence Service). (2024b). *CSIS Public Report 2023*. Ottawa, ON: CSIS. https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2023.html.

CSIS (Canadian Security Intelligence Service). (2024c). Five Eyes intelligence partners launch shared security advice initiative for tech companies, researchers, and investors. Retrieved May 2025, from https://www.canada.ca/en/security-intelligence-service/news/2024/10/five-eyes-intelligence-partners-launch-shared-security-advice-initiative-for-tech-companies-researchers-and-investors.html.

CSIS (Canadian Security Intelligence Service). (2024d). *Need to Know September 2024*. Ottawa, ON: CSIS. https://www.citt.ca/insights/resources/csis-september-2024.

CSIS (Canadian Security Intelligence Service). (2025). *CSIS Public Report 2024*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2024.html.

Cunningham, A. (2024, May 14). Shifting ice: How the Russian invasion of Ukraine has changed Arctic Circle governance and the Arctic Council's path forward. *The Arctic Institute—Center for Circumpolar Security Studies*. Retrieved November 2024, from https://www.thearcticinstitute.org/shifting-ice-russian-invasion-ukraine-arctic-circle-governance-arctic-councils-path-forward/.

Cyber Centre (Canadian Centre for Cyber Security). (2020). *Cyber Threat Bulletin: The Continued Impact of COVID-19 on Cyber Threat Activity*. Ottawa, ON: Government of Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-continued-impact-covid-19-cyber-threat-activity.

Cyber Centre (Canadian Centre for Cyber Security). (2024a). *The Cyber Threat to Research Laboratories*. Ottawa, ON: Government of Canada. https://www.cyber.gc.ca/en/guidance/cyber-threat-research-laboratories.

Cyber Centre (Canadian Centre for Cyber Security). (2024b). Security considerations for research and development organizations (ITSAP.00.130). Retrieved June 2025, from https://www.cyber.gc.ca/en/guidance/security-considerations-research-and-development-itsap00130.

Cyber Centre (Canadian Centre for Cyber Security). (2024c). *National Cyber Threat Assessment 2025–2026*. Ottawa, ON: Communications Security Establishment Canada. https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf.

d'Hooghe, I. & Lammertink, J. (2022). *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden, the Netherlands: Leiden Asia Centre & Netherlands Advisory Council for Science, Technology and Innovation. https://leidenasiacentre.nl/wp-content/uploads/2022/11/How-National-Governments-and-Research-Institutions-Safequard-Knowledge-Development-in-Science-and-Technology.pdf.

DAAD (German Academic Exchange Service Support). (n.d.). Kompetenzzentrum Internationale Wissenschaftskooperationen (KIWi) [Centre of Excellence for International Scientific Cooperation]. Retrieved August 2024, from https://www.daad.de/de/infos-services-fuer-hochschulen/kompetenzzentrum/.

Dao, T. K., Evans, K. M., Shannon, M. D., Bronk, C., Neuhauser, C., & Roberts, E. (2024). *Responsible Collaboration Through Appropriate Research Security: A Workshop To Discuss and Study the Emergent Discipline of Research on Research Security*. Houston,TX: Rice University's Baker Institute for Public Policy. https://www.bakerinstitute.org/research/responsible-collaboration-through-appropriate-research-security.

Davidson, P. (2017, December 1). Beyond the basics: Taking Canada–China collaboration to the next level. *Hill Times*. Retrieved May 2025, from https://univcan.ca/news/beyond-basics-taking-canada-china-collaboration-next-level/.

de Beer, J. (n.d.). Who has jurisdiction over intellectual property law and policy in Canada's federal system? Retrieved June 2025, from https://www.jeremydebeer.ca/intellectual-property-a-canadian-federalism/.

de Beer, J. & Dylan, D. (2015). Traditional knowledge governance challenges in Canada. In M. Rimmer (Ed.), *Indigenous Intellectual Property*. Cheltenham, United Kingdom: Edward Elgar Publishing.

De Bruijn, A. (2023, May 30). 'New knowledge security screening is counterproductive.' *Delta*. Retrieved August 2024, from https://delta.tudelft.nl/en/article/new-knowledge-security-screening-counterproductive.

Department for Science, Innovation & Technology. (2023). *RCAT update August 2023*. London, United Kingdom: Government of the United Kingdom. https://assets.publishing.service.gov.uk/media/654a2f1be2e16a000d42aae4/research_collaboration_advice_team_update_report.pdf.

DFO (Fisheries and Oceans Canada). (2022). About the Canadian Hydrographic Service. Retrieved May 2024, from https://www.charts.gc.ca/help-aide/about-apropos/index-eng.html#legal.

DiEuliis, D. & Giordano, J. (2017). Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. *Health Security*, *15*(3), 296–302. https://doi.org/10.1089/hs.2016.0120.

DLR (German Aerospace Center). (2022). *Annotated Collection of Guidance for Secure and Successful International R&I Cooperation*. Bonn, Germany: DLR. https://www.safeguarding-science.eu/wp-content/uploads/annotated-collection-2022.pdf.

DLR (German Aerospace Center). (2023). *Open Source Intelligence (OSINT) Application to Illustrate the Potential Compromise of Academic Knowledge Security Systems*. Bonn, Germany: DLR. https://www.safeguarding-science.eu/wp-content/uploads/OSINT_report_exec_sum-11-2023.pdf.

DLR (German Aerospace Center). (2024). *Due Diligence in Science*. Bonn, Germany: DLR. https://www.safeguarding-science.eu/wp-content/uploads/Due-Diligence-in-Science_Manual2024.pdf.

DND & CAF (Department of National Defence and Canadian Armed Forces). (2021). *DND/CAF Open Science Action Plan*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/open-science-action-plan.html.

DND (Department of National Defence). (2023). *Evaluation of the IDEaS Program*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/eval-ideas-program.html.

DND (Department of National Defence). (2024a). *IDEaS Annual Report 2022–2023*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/ideas-annual-report-2022-2023.html.

DND (Department of National Defence). (2024b). *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

DOD (Department of Defense). (2022). JASON Defense Advisory Panel reports. Retrieved September 2024, from https://irp.fas.org/agency/dod/jason/.

DOD (Department of Defense). (2023). *Policy for Risk-Based Security Reviews of Fundamental Research*. Washington, D.C.: DOD. https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF.

DORA (Declaration on Research Assessment). (2012). San Francisco Declaration on Research Assessment. Retrieved November 2024, from https://sfdora.org/read/.

DRDC (Defence Research and Development Canada). (2023). Research and development capabilities. Retrieved June 2024, from https://www.canada.ca/en/defence-research-development/services/capabilities.html.

EC (European Commission). (2019). Open science. Retrieved August 2024, from https://www.cesaer.org/content/10-library/2023/ec-rtd-factsheet-open-science-2019.pdf.

EC (European Commission). (2021a). *Commission Recommendation (EU) 2021/1700 of 15 September 2021 on Internal Compliance Programmes for Controls of Research Involving Dual-Use Items Under Regulation (EU) 2021/821 of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items*. Brussels, Belgium: Official Journal of the European Union. https://op.europa.eu/en/publication-detail/-/publication/a5b08317-1c07-11ec-b4fe-01aa75ed71a1/language-en.

EC (European Commission). (2021b). *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)*.

EC (European Commission). (2022). *Open Science and Intellectual Property Rights: How Can They Better Interact? State of the Art and Reflections*. Brussels, Belgium: Publications Office of the European Union. https://data.europa.eu/doi/10.2777/347305.

EC (European Commission). (2024a). *Council Recommendation on Enhancing Research Security*. Brussels, Belgium: EC. https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf.

EC (European Commission). (2024b). Fact sheet: Council recommendation on research security. Retrieved August 2024, from https://research-and-innovation.ec.europa.eu/document/download/09a49b8b-ddc8-43eb-856f-73ffbe5076c8_en?filename=ec_rtd_council-recommendation-research-security-fs.pdf.

EC (European Commission). (n.d.-a). Canada. Retrieved June 2025, from https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/bilateral-cooperation-science-and-technology-agreements-non-eu-countries/canada_en.

EC (European Commission). (n.d.-b). Trends for open access to publications. Retrieved September 2024, from https://web.archive.org/web/20240921011832/https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/open-science-monitor/trends-open-access-publications_en.

ECCC (Environment and Climate Change Canada). (2021). *Environment and Climate Change Canada Open Science Action Plan 2021–2026*. Gatineau, QC: Government of Canada. https://publications.gc.ca/collections/collection_2021/eccc/En4-446-2021-eng.pdf.

Eiterjord, T. (2023, November 23). What the 14th Five-Year Plan Says About China's Arctic Interests. *The Arctic Institute—Center for Circumpolar Security Studies*. Retrieved November 2024, from https://www.thearcticinstitute.org/14th-five-year-plan-chinas-arctic-interests/.

Eiterjord, T. (2024). Securitise the volume: Epistemic territorialisation and the geopolitics of China's Arctic research. *Territory, Politics, Governance*, *12*(1), 93–111. https://doi.org/10.1080/21622671.2023.2179535.

Engel-Glatter, S. & Ienca, M. (2018). Life scientists' views and perspectives on the regulation of dual-use research of concern. *Science and Public Policy*, *45*(1), 92–102. https://doi.org/10.1093/scipol/scx050.

Evan, W. M. & Hays, B. B. (2006). Dual-use technology in the context of the non-proliferation regime. *History and Technology*, *22*(1), 105–113. https://doi.org/10.1080/07341510500517850.

Evans, N. G. & Commins, A. (2017, February 2). Defining dual-use research: When scientific advances can both help and hurt humanity. *The Conversation*. Retrieved March 2024, from http://theconversation.com/defining-dual-use-research-when-scientific-advances-can-both-help-and-hurt-humanity-70333.

Evans, N. G., Selgelid, M. J., & Simpson, R. M. (2022). Reconciling regulation with scientific autonomy in dual-use research. *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, *47*(1), 72–94. https://doi.org/10.1093/jmp/jhab041.

Evans, P. (2022, September 19). Canadian universities & China: Research collaborations in question. *The Institute for Peace and Diplomacy*. Retrieved from https://peacediplomacy.org/2022/09/19/canadian-universities-china-research-collaborations-in-question/.

Falco, G., Boschetti, N., & Nikas, I. (2024). *Undercover Infrastructure: Dual-Use Arctic Satellite Ground Stations*. Waterloo, ON: Centre for International Governance Innovation. https://www.cigionline.org/publications/undercover-infrastructure-dual-use-arctic-satellite-ground-stations/.

FC (Federal Court). (2023a). *Jahantigh v Canada (Citizenship and Immigration)*, 2023 FC 1253.

FC (Federal Court). (2023b). *Li v Canada (Citizenship and Immigration)*, 2023 FC 1753.

Flagg, M. & Arnold, Z. (2021). *A New Institutional Approach to Research Security in the United States*. Washington, D.C.: Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states/.

FNIGC (First Nations Information Governance Centre). (2020). *A First Nations Data Governance Strategy*. Ottawa, ON: FNIGC. https://fnigc.ca/wp-content/uploads/2020/09/FNIGC_FNDGS_report_EN_FINAL.pdf.

FNIGC (First Nations Information Governance Centre). (2021). *The First Nation Data Centre (FNDC) On-Site Policies and Procedures Guide*. Ottawa, ON: FNIGC. https://fnigc.ca/wp-content/uploads/2022/01/FNDC_On-site-Policies-and-Procedures-Nov_2021.pdf.

FNIGC (First Nations Information Governance Centre). (2024). *A First Nations Guide to the Privacy Act*. Ottawa, ON: FNIGC. https://fnigc.ca/wp-content/uploads/2024/08/FNIGC_FN_Guide_Privacy_Act_EN-1.pdf.

FNIGC (First Nations Information Governance Centre). (n.d.). The First Nations Principles of OCAP®. Retrieved October 2022, from https://fnigc.ca/ocap-training/.

Franklin, A. R. (2025, January 29). How Rice is using generative AI to enhance research security, saving hundreds of expert hours each week. *Rice University*. Retrieved June 2025, from https://news.rice.edu/news/2025/how-rice-using-generative-ai-enhance-research-security-saving-hundreds-expert-hours-each.

FRQ (Fonds de recherche du Québec). (2020). Les Fonds de recherche du Québec adhèrent à la Déclaration de San Francisco sur l'évaluation de la recherche. Retrieved February 2024, from https://frq.gouv.qc.ca/les-fonds-de-recherche-du-quebec-adherent-a-la-declaration-de-san-francisco-sur-levaluation-de-la-recherche/.

FRQ (Fonds de recherche du Québec). (2022). *Politique de diffusion en libre accès (version révisée)*. Québec, QC: FRQ. https://frq.gouv.qc.ca/app/uploads/2022/06/politique-libre-acces-revisee_vf.pdf.

Fujii, Y., Rémy, E., Zuo, H., Oke, P., Halliwell, G., Gasparin, F., … Usui, N. (2019). Observing system evaluation based on ocean data assimilation and prediction systems: On-going challenges and a future vision for designing and supporting ocean observational networks. *Frontiers in Marine Science*, *6*, 417. https://doi.org/10.3389/fmars.2019.00417.

Funaiole, M. P., Hart, B., Bermudez Jr., J. S., & Powers-Riggs, A. (2023, April 18). Frozen frontiers: China's great power ambitions in the polar regions. *Center for Strategic and International Studies*. Retrieved May 2025, from https://features.csis.org/hiddenreach/china-polar-research-facility.

Gabel, C. & Henry, R. (2024). *National Métis Health Data Strategy and Principles*. Ottawa, ON: Métis National Council. https://macsphere.mcmaster.ca/bitstream/11375/30688/2/MNC_Final_Draft_Report_March_2024.pdf.

Gaffey, C. B., Bax, N., Krauzig, N., & Tougeron, K. (2024). A call to strengthen international collaboration to assess climate change effects in polar regions. *PLOS Climate*, *3*(10), e0000495. https://doi.org/10.1371/journal.pclm.0000495.

Gattolin, A. (2021). *Mission d'information "Influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences."* Paris, France: Senate of France. https://www.senat.fr/rap/r20-873/r20-8731.pdf.

GC (Government of Canada). (1982). *Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK)*, 1982, c 11.

GC (Government of Canada). (1985a). *Competition Act*, RSC 1985, c C-34.

GC (Government of Canada). (1985b). *Defence Production Act*, RSC 1985, c D-1.

GC (Government of Canada). (1985c). *Export and Import Permits Act*, RSC 1985, c E-19.

GC (Government of Canada). (1986). *Agreement between the Government of Canada and the Government of Japan on Cooperation in Science and Technology*. Ottawa, ON: GC. https://www.treaty-accord.gc.ca/text-texte.aspx?id=102070.

GC (Government of Canada). (1992). *Special Economic Measures Act*, SC 1992, c 17.

GC (Government of Canada). (1997). *Nuclear Safety and Control Act*, SC 1997, c 9.

GC (Government of Canada). (2001). *Immigration and Refugee Protection Act*, SC 2001, c 27.

GC (Government of Canada). (2008). *Canada–China agreement on scientific and technological cooperation*. Ottawa, ON: GC. https://www.canada.ca/en/environment-climate-change/corporate/international-affairs/partnerships-countries-regions/asia/canada-china-scientific-technological-cooperation.html.

GC (Government of Canada). (2009). *Human Pathogens and Toxins Act*, SC 2009, c 24.

GC (Government of Canada). (2010). *Nuclear Non-proliferation Import and Export Control Regulations*, SOR/2000-210.

GC (Government of Canada). (2016). *Controlled Goods Regulations*, SOR/2001-32.

GC (Government of Canada). (2019a). *Setting New Directions to Support Indigenous Research and Research Training in Canada*. Ottawa, ON: GC. https://www.canada.ca/en/research-coordinating-committee/priorities/indigenous-research/strategic-plan-2019-2022.html.

GC (Government of Canada). (2019b). Lab 101: What does it take to house the world's deadliest diseases? Retrieved January 2025, from https://science.gc.ca/site/science/en/blogs/science-health/lab-101-what-does-it-take-house-worlds-deadliest-diseases.

GC (Government of Canada). (2020). *Roadmap for Open Science*. Ottawa, ON: Office of the Chief Science Advisor. https://science.gc.ca/site/science/sites/default/files/attachments/2022/Roadmap-for-Open-Science.pdf.

GC (Government of Canada). (2021a). *Budget 2021: A Recovery Plan for Jobs, Growth, and Resilience*. Ottawa, ON: GC. https://publications.gc.ca/collections/collection_2021/fin/F1-23-3-2021-eng.pdf.

GC (Government of Canada). (2021b). Tri-Agency Research Data Management Policy. Retrieved August 2024, from https://science.gc.ca/site/science/en/interagency-research-funding/policies-and-guidelines/research-data-management/tri-agency-research-data-management-policy.

GC (Government of Canada). (2021c). *Export Control List*, SOR/89-202.

GC (Government of Canada). (2021d). Assessing your risk profile. Retrieved May 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/assessing-your-risk-profile.

GC (Government of Canada). (2021e). What are the risks? Retrieved March 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/what-are-risks.

GC (Government of Canada). (2021f). Who are you at risk from? Retrieved March 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/who-are-you-risk.

GC (Government of Canada). (2022a). Why safeguard your research? Retrieved March 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/why-safeguard-your-research.

GC (Government of Canada). (2022b). *Tri-Agency Framework: Responsible Conduct of Research (2021)*. Ottawa, ON: GC. https://rcr.ethics.gc.ca/eng/framework-cadre-2021.html.

GC (Government of Canada). (2022c). Canada First Research Excellence Fund: Application process—2022 competition. Retrieved February 2025, from https://www.cfref-apogee.gc.ca/program-programme/competitions-concours/2022/apply-demande-eng.aspx#2.6.

GC (Government of Canada). (2024a). *Canada's Arctic Foreign Policy*. Ottawa, ON: GC. https://www.international.gc.ca/gac-amc/publications/transparency-transparence/arctic-arctique/arctic-policy-politique-arctique.aspx?lang=eng.

GC (Government of Canada). (2024b). *Budget 2024—Fairness for Every Generation*. Ottawa, ON: GC. https://www.budget.canada.ca/2024/report-rapport/toc-tdm-en.html.

GC (Government of Canada). (2024c). Tri-Agency Research Data Management Policy—Frequently asked questions. Retrieved February 2025, from https://science.gc.ca/site/science/en/interagency-research-funding/policies-and-guidelines/research-data-management/tri-agency-research-data-management-policy-frequently-asked-questions.

GC (Government of Canada). (2024d). *Human Pathogens and Toxins Regulations*, SOR/2015-44.

GC (Government of Canada). (2024e). Research Support Fund. Retrieved February 2025, from https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-eng.aspx.

GC (Government of Canada). (2024f). Research security funding awarded in 2024-25. Retrieved June 2025, from https://www.rsf-fsr.gc.ca/apply-demande/grants-subventions/rs2024-eng.aspx.

GC (Government of Canada). (2024g). Case studies - Scenarios. Retrieved May 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/case-studies-scenarios.

GC (Government of Canada). (2024h). *A Guide to Canada's Export Control List—January 2024*. Ottawa, ON: GC. https://www.international.gc.ca/trade-commerce/assets/pdfs/guides/export-control-list-guide-2024-eng.pdf.

GC (Government of Canada). (2024i). Communications, capacity and outreach. Retrieved January 2025, from https://science.gc.ca/site/science/en/northern-contaminants-program/call-proposals-2025/northern-contaminants-program-2025-call-proposals#section9.

GC (Government of Canada). (2024j). Research Security Centre. Retrieved November 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/research-security-center.

GC (Government of Canada). (2024k). The Secretariat on Responsible Conduct of Research (SRCR). Retrieved June 2025, from https://rcr.ethics.gc.ca/eng/srcr-scrr_staff-personnel.html.

GC (Government of Canada). (2025a). Government of Canada finalizes investment to support Canadian-born AI leader, Cohere. Retrieved May 2025, from https://www.canada.ca/en/innovation-science-economic-development/news/2025/03/government-of-canada-finalizes-investment-to-support-canadian-born-ai-leader-cohere.html.

GC (Government of Canada). (2025b). Government of Canada and the duty to consult. Retrieved January 2025, from https://www.rcaanc-cirnac.gc.ca/eng/1331832510888/1609421255810.

GC (Government of Canada). (2025c). Operational ocean-ice forecasting. Retrieved May 2024, from https://science.gc.ca/site/science/en/concepts/operational-ocean-ice-forecasting.

GC (Government of Canada). (2025d). Oceans Protection Plan. Retrieved June 2025, from https://tc.canada.ca/en/campaigns/protecting-our-coasts-oceans-protection-plan.

GC (Government of Canada). (2025e). 2025 provincial and territorial allocations under the international student cap. Retrieved June 2025, from https://www.canada.ca/en/immigration-refugees-citizenship/news/notices/2025-provincial-territorial-allocations-under-international-student-cap.html.

GC (Government of Canada). (2025f). *A Guide to Canada's Export Controls List*. Ottawa, ON: Global Affairs Canada. https://www.international.gc.ca/trade-commerce/assets/pdfs/guides/export-control-list-guide-2025-eng.pdf.

GC (Government of Canada). (2025g). Sensitive Technology List. Retrieved June 2025, from https://www.canada.ca/en/services/defence/nationalsecurity/sensitive-technology-list.html.

GC (Government of Canada). (2025h). Order Amending the Export Control List: SOR/2025-89. Retrieved June 2025, from https://gazette.gc.ca/rp-pr/p2/2025/2025-03-26/html/sor-dors89-eng.html.

GC (Government of Canada). (2025i). Backgrounder: Amendment to A Guide to Canada's Export Control List. Retrieved June 2025, from https://www.international.gc.ca/trade-commerce/controls-controles/ecl-lec/backgrounder-document-information-2025.aspx?lang=eng.

GC (Government of Canada). (2025j). Risk assessment review process. Retrieved February 2025, from https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships/national-security-guidelines-research-partnerships-risk-assessment-form/risk-assessment-review-process.

GC (Government of Canada). (2025k). Canada Research Chairs: Method of allocating Chairs. Retrieved May 2025, from https://www.chairs-chaires.gc.ca/program-programme/allocation-attribution-eng.aspx.

GC (Government of Canada). (2025l). Research Support Fund: Grant calculations. Retrieved May 2025, from https://www.rsf-fsr.gc.ca/apply-demande/calculations-eng.aspx.

Genome Canada. (2024a). *2023–24 Annual Report: Harnessing Genomics for Impact*. Ottawa, ON: Genome Canada. https://genomecanada.ca/wp-content/uploads/2024/07/GC-AnnualReport-2023-24_EN_web.pdf.

Genome Canada. (2024b). *Research Security Plan*. Ottawa, ON: Genome Canada. https://genomecanada.ca/wp-content/uploads/2024/12/Research-Security-Plan-2024-Dec.pdf.

Geremia, S. (2024, March 18). New research grants to bolster Canada's AI ecosystem. *Google Canada*. Retrieved November 2024, from https://blog.google/intl/en-ca/company-news/outreach-initiatives/new-research-grants-to-bolster-canadas-ai-ecosystem/.

GFW (Global Fishing Watch). (n.d.). Home. Retrieved June 2025, from https://globalfishingwatch.org/.

GHS Index (Global Health Security Index). (2021). 2021 GHS Index country profile for Canada. Retrieved May 2025, from https://ghsindex.org/country/canada/.

GIDA (Global Indigenous Data Alliance). (n.d.). CARE Principles for Indigenous Data Governance. Retrieved January 2025, from https://www.gida-global.org/care.

Global BioLabs. (2023). *Global BioLabs Report 2023*. London, United Kingdom: King's College London. https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf.

GlycoNet (Canadian Glycomics Network). (n.d.). Research security. Retrieved March 2025, from https://canadianglycomics.ca/research/research-security/.

Goodchild, M., Khair, S., Leahey, A., Newson, K., & Wilson, L. (2023). Research data sharing and reuse in Canada: Practice and policy. In K. Thompson, E. Hill, E. Carlisle-Johnston, D. Dennie, & E. Fortin (Eds.), *Research Data Management in the Canadian Context: A Guide for Practitioners and Learners* (1st ed.). London, ON: Western University, Western Libraries.

GOOS (Global Ocean Observing System). (n.d.). What we do. Retrieved November 2024, from https://goosocean.org/what-we-do/.

Gov. of AB (Government of Alberta). (2024). *Research Capacity Program*. Edmonton, AB: Gov. of Alberta. https://open.alberta.ca/dataset/faf898eb-ed6b-4fae-ae39-f2aa7efcf6d2/resource/5460ea77-829e-4dcc-b5d8-2173308df567/download/ti-research-capacity-program-guidelines-2024-2025.pdf.

Gov. of Australia (Government of Australia). (2013). *Security Sensitive Biological Agent (SSBA) Standards*. Canberra, Australia: Gov. of Australia. https://www.health.gov.au/sites/default/files/documents/2022/06/ssba-standards.pdf.

Gov. of Australia (Government of Australia). (2018). Foreign Influence Transparency Scheme Act 2018.

Gov. of Australia (Government of Australia). (2020). *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* No. 116.

Gov. of Australia (Government of Australia). (2021). *Australia's Foreign Relations (State and Territory Arrangements) Act 2020: Fact Sheet 4 – Australian Universities*. Canberra, Australia: Department of Foreign Affairs and Trade. https://www.foreignarrangements.gov.au/resources/fact-sheets.

Gov. of Australia (Government of Australia). (2023). List of critical technologies in the national interest. Retrieved September 2024, from https://www.industry.gov.au/publications/list-critical-technologies-national-interest.

Gov. of Australia (Government of Australia). (2024). Security Sensitive Biological Agents (SSBA) Regulatory Scheme. Retrieved August 2024, from https://www.health.gov.au/our-work/ssba-regulatory-scheme.

Gov. of Australia (Government of Australia). (2025). National Counter Foreign Interference Coordinator. Retrieved September 2024, from https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference.

Gov. of France (Government of France). (1990). *Code pénal*.

Gov. of France (Government of France). (2012). *Circulaire interministerielle de mise en oeuvre du dispositif de protection du potentiel scientifique et technique de la nation*. Paris, France: SGDSN. https://www.legifrance.gouv.fr/download/pdf/circ?id=36329.

Gov. of France (Government of France). (2020). *Décret n° 2020-1481 du 30 novembre 2020 portant mesure nationale autorisée par le paragraphe 3 de l'article 6 du règlement (CE) no 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage*.

Gov. of France (Government of France). (2024). *Arrêté du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies associés à l'ordinateur quantique et à ses technologies habilitantes et d'équipements de conception, développement, production, test et inspection de composants électroniques avancés*.

Gov. of Germany (Government of Germany). (1949). *Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 19 December 2022 (Federal Law Gazette I p. 2478)*.

Gov. of Japan (Government of Japan). (2023). *Checklist for New Risks Associated with Increasing Internationalization and Openness of Research (Template)*. Tokyo, Japan: Cabinet Office. https://www8.cao.go.jp/cstp/english/doc/checklist_for_univ_en.pdf.

Gov. of Netherlands (Government of the Netherlands). (2022). *National Knowledge Security Guidelines: Secure International Collaboration*. The Hague, the Netherlands: Gov. of Netherlands. https://english.loketkennisveiligheid.nl/site/binaries/site-content/collections/documents/2022/04/07/national-knowledge-security-guidelines/National+Knowledge+Security+Guidelines.pdf.

Gov. of Netherlands (Government of the Netherlands). (2023). *Besluit toepassingsbereik sensitieve technologie*.

Gov. of Netherlands (Government of the Netherlands). (2025). Screening for researchers wis[h]ing to handle sensitive knowledge. Retrieved June 2025, from https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-sensitive-knowledge.

Gov. of New Zealand (Government of New Zealand). (2020). *Trusted Research: Guidance for Institutions and Researchers*. Wellington, New Zealand: Centre for the Protection of National Infrastructure, Science New Zealand & Universities New Zealand. https://www.protectivesecurity.govt.nz/assets/protective-security-requirements/resources/psr-trusted-research-guidance-spreads.pdf.

Gov. of New Zealand (Government of New Zealand). (2022). *Due Diligence Assessments for Espionage and Foreign Interference Threats*. Wellington, New Zealand: Protective Security Requirements. https://www.protectivesecurity.govt.nz/assets/protective-security-requirements/resources/psr-due-diligence-assessments.pdf.

Gov. of New Zealand (Government of New Zealand). (2024). *New Zealand Strategic Goods List*. Wellington, New Zealand: Ministry of Foreign Affairs and Trade. https://www.mfat.govt.nz/assets/Trade-General/Brokering-weapons-AND-Trading-weapons-and-controlled-chemicals/NZ-Strategic-Goods-List-November.pdf.

Gov. of ON (Government of Ontario). (2023). *Mitigating Economic and Geopolitical Risk Checklist for Ontario Research Fund Applications*. Toronto, ON: Gov. of ON. https://forms.mgcs.gov.on.ca/en/dataset/on00352.

Gov. of ON (Government of Ontario). (2024a). *Research Security Guidelines for Ontario Research Funding Programs*. Toronto, ON: Ministry of Colleges and Universities. https://forms.mgcs.gov.on.ca/en/dataset/on00708.

Gov. of ON (Government of Ontario). (2024b). *Application Attestation Form for Researchers Applying to the Ontario Research Funding Programs*. Toronto, ON: Ministry of Colleges and Universities. https://forms.mgcs.gov.on.ca/en/dataset/on00694.

Gov. of QC (Government of Quebec). (2024a). *Act Respecting Protection Against Reprisals Related to the Disclosure of Wrongdoings* P-33.01.

Gov. of QC (Government of Quebec). (2024b). *Act to Facilitate the Disclosure of Wrongdoings Relating to Public Bodies* D-11.1.

Gov. of South Korea (Government of South Korea). (2023). *Act on Protection of Industrial Technology*.

Gov. of United Kingdom (Government of the United Kingdom). (2024). National Security and Investment Act: Details of the 17 types of notifiable acquisitions. Retrieved June 2025, from https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions.

Gov. of United Kingdom (Government of the United Kingdom). (2025). Academic Technology Approval Scheme (ATAS). Retrieved August 2024, from https://www.gov.uk/guidance/academic-technology-approval-scheme.

Gov. of United Kingdom (Government of the United Kingdom). (n.d.). Engineering Biology Responsible Innovation Advisory Panel. Retrieved May 2025, from https://www.gov.uk/government/groups/engineering-biology-responsible-innovation-advisory-panel.

Gov. of United States (Government of the United States). (1991). *Protection of Human Subjects*, 45 CFR 46.

Gov. of United States (Government of the United States). (2022a). *National Strategy for the Arctic Region*. Washington, D.C.: Gov. of United States. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf.

Gov. of United States (Government of the United States). (2022b). *CHIPS and Science Act* PL 117-167.

Gov. of United States (Government of the United States). (2024a). *United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential*. Washington, D.C.: Gov. of United States. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/USG-Policy-for-Oversight-of-DURC-and-PEPP.pdf.

Gov. of United States (Government of the United States). (2024b). *Implementation Guidance for the United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential*. Washington, D.C.: Gov. of United States. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/USG-DURC-PEPP-Implementation-Guidance.pdf.

Gownaris, N. J., Vermeir, K., Bittner, M.-I., Gunawardena, L., Kaur-Ghumaan, S., Lepenies, R., … Zakari, I. S. (2022). Barriers to full participation in the open science life cycle among early career researchers. *Data Science Journal*, *21*(2), 1–15. https://doi.org/10.5334/dsj-2022-002.

Grewal, S. (2022). International students for long-term prosperity in Canadian economy: Expanding pathways to permanence for international students in Canada. *Crossings: An Undergraduate Arts Journal*, *2*, 140–146. https://doi.org/10.29173/crossings45.

Gryphon Scientific, LLC. (2023). *Characterizing Private-Sector Research on Human Pathogens in the United States*. Takoma Park, MD: Gryphon Scientific, LLC. https://pandorareport.org/wp-content/uploads/2023/10/private-sector-research-final.pdf.

Gunashekar, S., d'Angelo, C., Flanagan, I., Motsi-Omoijiade, D., Virdee, M., Feijao, C., & Porter, S. (2022). *Using Quantum Computers and Simulators in the Life Sciences: Current Trends and Future Prospects*. Cambridge, United Kingdom: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1899-1.html.

Hähnel, M. (2024). Conceptualizing dual use: A multidimensional approach. *Research Ethics*, *21*(2), 205–227. https://doi.org/10.1177/17470161241261466.

Harlan, T. (2019, October 25). State of sensitivity: Navigating fieldwork in an increasingly authoritarian China. *Made in China Journal*. Retrieved June 2025, from https://madeinchinajournal.com/2019/10/25/state-of-sensitivity-navigating-fieldwork-in-an-increasingly-authoritarian-china/.

HC & PHAC (Health Canada and Public Health Agency of Canada). (2022). *Evaluation of the Human Pathogens and Toxins Act and Regulations Framework 2015–16 to 2020–21*. Ottawa, ON: Government of Canada Office of Audit and Evaluation. https://www.canada.ca/en/public-health/corporate/transparency/corporate-management-reporting/evaluation/human-pathogens-toxins-act-regulations-framework-2015-2016-2020-2021.html.

Heathershaw, J., Chalcraft, J., Chubb, A., Fulda, A., Hughes, C., Kaczmarska, K., … Yıldız, Y. Y. (2022). Model code of conduct: Protection of academic freedom and the academic community in the context of the internationalisation of the UK HE sector. *The International Journal of Human Rights*, 26(10), 1858–1865. https://doi.org/10.1080/13642987.2022.2148977.

Heaven, W. D. (2023, May 12). The open-source AI boom is built on Big Tech's handouts. How long will it last? *MIT Technology Review*. Retrieved November 2024, from https://www.technologyreview.com/2023/05/12/1072950/open-source-ai-google-openai-eleuther-meta/.

HEC Montréal (Hautes études commerciales de Montréal). (2023). *Politique sur la sécurité des activités à l'international*. Montréal, QC: HEC Montréal. https://www.hec.ca/direction_services/secretariat_general/juridique/reglements_politiques/documents/politique-securite-activites-international.pdf.

Heikkilä, M. (2024, October 18). The race to find new materials with AI needs more data. Meta is giving massive amounts away for free. *MIT Technology Review*. Retrieved November 2024, from https://www.technologyreview.com/2024/10/18/1105880/the-race-to-find-new-materials-with-ai-needs-more-data-meta-is-giving-massive-amounts-away-for-free/.

Heininen, L., Everett, K., Padrtova, B., & Reissell, A. (2020). *Arctic Policies and Strategies — Analysis, Synthesis, and Trends*. Laxenburg, Austria: International Institute for Applied Systems Analysis. https://pure.iiasa.ac.at/id/eprint/16175/1/ArticReport_WEB_new.pdf.

Helmholtz (Helmholtz Association of German Research Centres). (n.d.). Research security in international scientific collaborations. Retrieved August 2024, from https://www.helmholtz.de/en/international/research-security/.

HHS, CDC, & USDA (U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, and U.S. Department of Agriculture, Animal and Plant Health Inspection Service). (2020). *2019 Annual Report of the Federal Select Agent Program*. Washington, D.C.: HHS, CDC, & USDA. https://www.selectagents.gov/resources/publications/docs/FSAP_Annual_Report_2019_508.pdf.

HHS, CDC, & USDA (U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, and U.S. Department of Agriculture, Animal and Plant Health Inspection Service). (2024). *2023 Annual Report of the Federal Select Agent Program*. Washington, D.C.: HHS, CDC, & USDA. https://www.selectagents.gov/resources/publications/docs/FSAP-Annual-Report-2023_508.pdf.

Himmel, M. (2023). *Biosecurity Risk Assessment in the Life Sciences: Towards a Toolkit for Individual Practitioners*. Stockholm, Sweden: Stockholm International Peace Research Institute. https://www.sipri.org/publications/2023/other-publications/biosecurity-risk-assessment-life-sciences-towards-toolkit-individual-practitioners.

Holbrook, D. (1995). Government support of the semiconductor industry: Diverse approaches and information flows. *Business and Economic History*, *24*(2), 133–165. https://www.jstor.org/stable/23703131.

Huising, R. (2019). Pragmatic regulatory design: The case of human pathogens and toxins regulations in Canada. *Entreprises et histoire*, *97*(4), 58–69. https://doi.org/10.3917/eh.097.0058.

Huising, R. & Silbey, S. S. (2018). From nudge to culture and back again: Coalface governance in the regulated organization. *Annual Review of Law and Social Science*, *14*, 91–114. https://doi.org/10.1146/annurev-lawsocsci-110615-084716.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 2053951720982012. https://doi.org/10.1177/2053951720982012.

IARPC (Interagency Arctic Research Policy Committee). (2021). *Arctic Research Plan 2022–2026*. Washington, D.C.: National Science and Technology Council, Office of Science and Technology Policy. https://www.iarpccollaborations.org/plan/index.html.

IHO (International Hydrographic Organization). (2021). About the IHO. Retrieved May 2024, from https://iho.int/en/about-the-iho.

IHRC (Ittaq Heritage & Research Centre). (n.d.). Research. Retrieved June 2025, from https://ittaq.ca/research/.

Indigenous Advisory Circle & SSHRC (Social Sciences and Humanities Research Council). (2025). Indigenous research. Retrieved January 2025, from https://sshrc-crsh.canada.ca/en/funding/terminology.aspx#11.

Inglesby, T. (2024, May 7). Take-aways from strong new OSTP policy on DURC and pathogens with pandemic potential. *LinkedIn*. Retrieved August 2024, from https://www.linkedin.com/pulse/take-aways-from-strong-new-ostp-policy-durc-pathogens-tom-inglesby-3lrje.

IPCC (Intergovernmental Panel on Climate Change). (2019). Summary for policymakers. In H.-O. Pörtner, D.C. Roberts, V. Masson-Delmotte, P. Zhai, M. Tignor, E. Poloczanska, … N.M. Weyer (Eds.), *The Ocean and Cryosphere in a Changing Climate: Special Report of the Intergovernmental Panel on Climate Change* (1st ed.). Cambridge, United Kingdom and New York, NY: Cambridge University Press.

ISC (International Science Council). (n.d.). *The International Science Council's Interpretation of the Right to Participate in and Benefit from Science*. Paris, France: ISC. https://council.science/wp-content/uploads/2024/11/The-Right-to-Participate-in-and-Benefit-from-Science_ISC.pdf.

ISED (Innovation, Science and Economic Development Canada). (2016). Tri-Agency Open Access Policy on Publications (2015). Retrieved June 2024, from https://ised-isde.canada.ca/site/science/en/interagency-research-funding/policies-and-guidelines/open-access/tri-agency-open-access-policy-publications-2015.

ISED (Innovation, Science and Economic Development Canada). (2021). Government of Canada takes action to protect Canadian research and intellectual property. Retrieved June 2025, from https://www.canada.ca/en/innovation-science-economic-development/news/2021/07/government-of-canada-takes-action-to-protect-canadian-research-and-intellectual-property.html.

ISED (Innovation, Science and Economic Development Canada). (2022a). *Canada's National Quantum Strategy*. Ottawa, ON: Government of Canada. https://ised-isde.canada.ca/site/national-quantum-strategy/sites/default/files/attachments/2022/NQS-SQN-eng.pdf.

ISED (Innovation, Science and Economic Development Canada). (2022b). *Open Source Due Diligence Summary*. Ottawa, ON: Government of Canada. https://ised-isde.canada.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-conducting-open-source-due-diligence/open-source-due-diligence-summary.

ISED (Innovation, Science and Economic Development Canada). (2022c). *Conducting Open Source Due Diligence for Safeguarding Research Partnerships*. Ottawa, ON: Government of Canada. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-conducting-open-source-due-diligence/conducting-open-source-due-diligence-safeguarding-research-partnerships.

ISED (Innovation, Science and Economic Development Canada). (2023a). *National Security Guidelines for Research Partnerships*. Ottawa, ON: Government of Canada. https://science.gc.ca/site/science/sites/default/files/documents/national_security_guidelines_for_research_partnerships_Jan2024.pdf.

ISED (Innovation, Science and Economic Development Canada). (2023b). *Sensitive Technology Research Areas*. Ottawa, ON: ISED. https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1081-sensitive-technology-research-areas-09Jan2024.pdf.

ISED (Innovation, Science and Economic Development Canada). (2023c). *Progress Report on the Implementation of Canada's National Security Guidelines for Research Partnerships and Supporting Research Security Efforts*. Ottawa, ON: Government of Canada. https://science.gc.ca/site/science/sites/default/files/documents/2023-11/1077-progress-report-2021-2023-23nov2023.pdf.

ISED (Innovation, Science and Economic Development Canada). (2023d). The presidents of Canada's federal research granting agencies announce a review of the Tri-Agency Open Access Policy on Publications. Retrieved November 2024, from https://science.gc.ca/site/science/en/interagency-research-funding/policies-and-guidelines/open-access/presidents-canadas-federal-research-granting-agencies-announce-review-tri-agency-open-access-policy.

ISED (Innovation, Science and Economic Development Canada). (2023e). *Named Research Organizations*. Ottawa, ON: Government of Canada. https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1082-named-research-organizations-list-09Jan2024.pdf.

ISED (Innovation, Science and Economic Development Canada). (2023f). *Policy on Sensitive Technology Research and Affiliations of Concern*. Ottawa, ON: Government of Canada. https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1154-policy-strac-en-final-09Jan2024.pdf.

ISED (Innovation, Science and Economic Development Canada). (2024a). National Security Guidelines for Research Partnerships' Risk Assessment Form. Retrieved May 2024, from https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships/national-security-guidelines-research-partnerships-risk-assessment-form.

ISED (Innovation, Science and Economic Development Canada). (2024b). Case Studies: How a security breach can impact your research. Retrieved January 2025, from https://ised-isde.canada.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/case-studies-how-security-breach-can-impact-your-research.

ISED (Innovation, Science and Economic Development Canada). (2024c). Tri-Agency Open Access Policy on Publications: Policy review survey results. Retrieved June 2024, from https://ised-isde.canada.ca/site/science/en/interagency-research-funding/policies-and-guidelines/open-access/tri-agency-open-access-policy-publications-policy-review-survey-results.

ISED (Innovation, Science and Economic Development Canada). (2025). Innovation, Science and Economic Development Canada's 2024–2025 Departmental Plan. Retrieved June 2025, from https://ised-isde.canada.ca/site/planning-performance-reporting/en/departmental-plans/innovation-science-and-economic-development-canadas-2024-2025-departmental-plan.

ISO (International Organization for Standardization). (2018). *ISO 31000:2018 Risk Management — Guidelines*. Geneva, Switzerland: ISO. https://www.iso.org/standard/65694.html.

ITK (Inuit Tapiriit Kanatami). (2018). *National Inuit Strategy on Research*. Ottawa, ON: ITK. https://www.itk.ca/wp-content/uploads/2020/10/ITK-National-Inuit-Strategy-on-Research.pdf.

ITK & NRI (Inuit Tapiriit Kanatami and Nunavut Research Institute). (2007). *Negotiating Research Relationships with Inuit Communities: A Guide for Researchers*. Ottawa, ON & Iqaluit, NU: ITK & NRI. https://itk.ca/wp-content/uploads/2016/07/Negotitiating-Research-Relationships-Researchers-Guide_0.pdf.

Iverson, S. J., Fisk, A. T., Hinch, S. G., Mills Flemming, J., Cooke, S. J., & Whoriskey, F. G. (2019). The Ocean Tracking Network: Advancing frontiers in aquatic science and management. *Canadian Journal of Fisheries and Aquatic Sciences*, *76*, 1041–1051. https://doi.org/10.1139/cjfas-2018-0481.

Jakob, U., Kraemer, F., Kraus, F., & Lengauer, T. (2024). Applying ethics in the handling of dual use research: The case of Germany. *Research Ethics*, *21*(2), 228–244. https://doi.org/10.1177/17470161241261044.

Jamal, M. (2022, April 27). ITK looking to make it easier for organizations to share information across Inuit Nunangat. *Nunatsiaq News*. Retrieved June 2023, from https://nunatsiaq.com/stories/article/itk-looking-to-make-it-easier-for-organizations-to-share-information-across-inuit-nunangat/.

JASON. (2019). *Fundamental Research Security*. McLean, VA: MITRE Corporation. https://nsf-gov-resources.nsf.gov/files/JSR-19-2IFundamentalResearchSecurity-12062019FINAL.pdf.

JASON. (2024). *Safeguarding the Research Enterprise*. McLean, VA: MITRE Corporation. https://nsf-gov-resources.nsf.gov/files/JSR-23-12-Safeguarding-the-Research-Enterprise-Final.pdf?VersionId=ZVhvRaTIrxMsdZql6E_yz5pN6Sswo fSl.

Jin, X., Xu, L., Xin, Y., & Adhikari, A. (2022). Political governance in China's state-owned enterprises. *China Journal of Accounting Research*, *15*, 100236. https://doi.org/10.1016/j.cjar.2022.100236.

JUS (Justice Canada). (2021). Backgrounder: United Nations Declaration on the Rights of Indigenous Peoples Act. Retrieved April 2024, from https://www.justice.gc.ca/eng/declaration/about-apropos.html.

Kavouras, P. & Charitidis, C. A. (2019). Dual use in modern research: Taming the Janus of technological advance. In R. Iphofen (Ed.), *Handbook of Research Ethics and Scientific Integrity*. Cham, Switzerland: Springer International Publishing.

KNAW, NFU, NWO, TO2-federatie, Vereniging Hogescholen, & VSNU (Royal Netherlands Academy of Arts and Sciences, Netherlands Federation of University Medical Centres, Netherlands Organisation for Scientific Research, Associated Applied Research Institutes, Association of Universities in the Netherlands, and Netherlands Association of Universities of Applied Sciences). (2018). *Netherlands Code of Conduct for Research Integrity*. n.l.: KNAW, NFU, NWO, TO2-federatie, Vereniging Hogescholen & VSNU. https://easy.dans.knaw.nl/ui/datasets/id/easy-dataset:110600.

KNAW (Royal Netherlands Academy of Arts and Sciences). (2023). *Knowledge Security: Academy Position Paper.* Amsterdam, the Netherlands: KNAW. https://www.knaw.nl/en/publications/knowledge-security-academy-position-paper.

Konczi, A. E. & Bill, L. (2024). Advancing First Nations Principles of OCAP®. In G. Garvey (Ed.), *Indigenous and Tribal Peoples and Cancer.* Cham: Springer Nature Switzerland.

Kosal, M. E. (2020a). Emerging life sciences and possible threats to international security. *Orbis*, *64*(4), 599–614. https://doi.org/10.1016/j.orbis.2020.08.008.

Kosal, M. E. (2020b). CRISPR and new genetic-engineering techniques: Emerging challenges to strategic stability and nonproliferation. *Nonproliferation Review*, *27*(4–6), 389–408. https://doi.org/10.1080/10736700.2020.1879464.

Kosal, M. E. & Huang, J. Y. (2015). Security implications and governance of cognitive neuroscience: An ethnographic survey of researchers. *Politics and the Life Sciences*, *34*(1), 93–108. https://doi.org/10.1017/pls.2015.4.

Kukutai, T. & Taylor, J. (2016). Data sovereignty for Indigenous Peoples: Current practice and future needs. In T. Kukutai & J. Taylor (Eds.), *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australia: Australian National University Press.

Lamb, C. & Munro, D. (2020). *The Intangible Shift: Changing Gears to Compete in the New Economy.* Toronto, ON: Brookfield Institute for Innovation+Entrepreneurship. https://brookfieldinstitute.ca/wp-content/uploads/2023/10/The-Intangible-Shift-ONLINE-1.pdf.

Lane, I. F. (2007). Change in higher education: Understanding and responding to individual and organizational resistance. *Journal of Veterinary Medical Education*, *34*(2), 85–92. https://doi.org/10.3138/jvme.34.2.85.

Larivière, V. & Sugimoto, C. R. (2018). Do authors comply when funders enforce open access to research? *Nature*, *562*(7728), 483–486. https://doi.org/10.1038/d41586-018-07101-w.

Laucht, C. (2012). *Elemental Germans: Klaus Fuchs, Rudolf Peierls and the Making of British Nuclear Culture 1939–59.* New York, NY: Palgrave Macmillan.

Leibniz Association. (2021). *Risk Management in International Scientific Collaboration.* Berlin, Germany: Leibniz Association. https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/%C3%9Cber_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf.

Leonard, K., Buttigieg, P. L., Hudson, M., Paul, K., Pearlman, J., & Juniper, S. K. (2022). Two-eyed seeing: Embracing the power of Indigenous knowledge for a healthy and sustainable Ocean. *PLOS Biology*, *20*(10), e3001876. https://doi.org/10.1371/journal.pbio.3001876.

Leopoldina & DFG (German National Academy of Sciences Leopoldina and German Research Foundation). (2022a). *The Handling of Security-Relevant Research in Germany—An Overview*. Berlin, Germany: Joint Committee on the Handling of Security-Relevant Research. https://www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/10/The-Handling-of-Security-Relevant-Research-in-Germany-An-Overview.pdf.

Leopoldina & DFG (German National Academy of Sciences Leopoldina and German Research Foundation). (2022b). *Scientific Freedom and Scientific Responsibility: Recommendations for Handling of Security-Relevant Research*. Halle, Germany: Leopoldina & DFG. https://www.dfg.de/resource/blob/176010/0f6dbcaa5e6b5b032bc24772cbf73a83/empfehlungen-de-en-data.pdf.

Leopoldina & DFG (German National Academy of Sciences Leopoldina and German Research Foundation). (n.d.-a). Frequently asked questions about security-relevant research and the KEFs. Retrieved August 2024, from https://www.security-relevant-research.org/faq-eng/.

Leopoldina & DFG (German National Academy of Sciences Leopoldina and German Research Foundation). (n.d.-b). Research assessment and international collaborations. Retrieved August 2024, from https://www.security-relevant-research.org/research/.

Lev, O. (2019). Regulating dual-use research: Lessons from Israel and the United States. *Journal of Biosafety and Biosecurity*, *1*, 80–85. https://doi.org/10.1016/j.jobb.2019.06.001.

Libman, A., Stone, R. W., & Vinokurov, E. (2022). Russian power and the state-owned enterprise. *European Journal of Political Economy*, *73*, 102122. https://doi.org/10.1016/j.ejpoleco.2021.102122.

Lipunov, N. & Devyatkin, P. (2023, May 30). The Arctic in the 2023 Russian Foreign Policy Concept. *The Arctic Institute—Center for Circumpolar Security Studies*. Retrieved November 2024, from https://www.thearcticinstitute.org/arctic-2023-russian-foreign-policy-concept/.

Loft, T. & Saumweber, W. (2020, April 22). Are we moving toward an ocean data dystopia? *Stephenson Ocean Security Project*. Retrieved November 2024, from https://ocean.csis.org/commentary/are-we-moving-toward-an-ocean-data-dystopia/.

Lukasik, S. (2011). Why the Arpanet was built. *IEEE Annals of the History of Computing*, *33*, 4–21. https://doi.org/10.1109/MAHC.2010.11.

MacIntyre, C. R., Adam, D. C., Turner, R., Chughtai, A. A., & Engells, T. (2020). Public awareness, acceptability and risk perception about infectious diseases dual-use research of concern: A cross-sectional survey. *BMJ Open*, *10*, e029134. https://doi.org/10.1136/bmjopen-2019-029134.

Major, R. M., Davis, A. M., Henderson, G. E., Inamine, G., & Conley, J. M. (2024). The public–private research ecosystem in the genome editing era. *iScience*, *27*, 109896. https://doi.org/10.1016/j.isci.2024.109896.

Malik, M., Agudelo, E., & Kunjwal, R. (2022). Quantum researcher mobility: The wonderful wizard of Oz who paid for Dorothy's visa fees. *Quantum Science and Technology*, 7, 034005. https://doi.org/10.1088/2058-9565/ac77b3.

Malone, M. (2021). Consequences of the criminalization of trade secret theft in Canada. *UBC Law Review*, 54(3), 889–933. https://commons.allard.ubc.ca/ubclawreview/vol54/iss3/7.

Marwaha, S., Timlin, J., Dickson, L., Kagiri-Kalanzi, E., & Johnson, J. (2023). *Complex Collaborations: Efficiency, Equity, Quality and Security in International Research*. Stow-cum-Quy, United Kingdom: Association of Research Managers and Administrators. https://arma.ac.uk/wp-content/uploads/2023/03/Trusted-Report_Booklet_v7.pdf.

MESR (French Ministry of Higher Education and Research). (2021). *Second French Plan for Open Science: Generalizing Open Science in France 2021–2024*. Paris, France: MESR. https://www.ouvrirlascience.fr/wp-content/uploads/2021/10/Second_French_Plan-for-Open-Science_web.pdf.

MESR (French Ministry of Higher Education and Research). (2023). French Open Science Monitor. Retrieved November 2024, from https://frenchopensciencemonitor.esr.gouv.fr/.

Mitacs. (2023). *Research Security Plan*. Montréal, QC: Mitacs. https://www.mitacs.ca/research-security/.

Moher, D. & Cobey, K. D. (2021). Ensuring the success of data sharing in Canada. *FACETS*, *6*, 1534–1538. https://doi.org/10.1139/facets-2021-0031.

Molloy, G. & Johnson, E. (2025, May 7). Investigation: Uncovering Chinese academic espionage at Stanford. *The Stanford Review*. Retrieved May 2025, from https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/.

Moran, K., Juniper, S. K., Bligh, S., Loock, D., Kulin, I., Paulson, M., & Pirenne, B. (2022). Canada's internet-connected ocean. *Frontiers in Marine Science*, *8*, 805134. https://doi.org/10.3389/fmars.2021.805134.

Morris, N. (2020, September 9). Why unis are worried about a federal power to cancel their foreign 'arrangements.' *The Conversation*. Retrieved January 2025, from http://theconversation.com/why-unis-are-worried-about-a-federal-power-to-cancel-their-foreign-arrangements-145689.

Moskovkin, V. M., Saprykina, T. V., Sadovski, M. V., & Serkina, O. V. (2021). International movement of open access to scientific knowledge: A quantitative analysis of country involvement. *The Journal of Academic Librarianship*, 47, 102296. https://doi.org/10.1016/j.acalib.2020.102296.

Mowery, D. C. (2010). Military R&D and innovation. In B.H. Hall & N. Rosenberg (Eds.), *Handbook of the Economics of Innovation*. Amsterdam, the Netherlands: North-Holland.

MPG (Max Planck Society). (2017). *Guidelines and Rules of the Max Planck Society on a Responsible Approach to Freedom of Research and Research Risks*. Munich, Germany: MPG. https://www.mpg.de/197392/researchFreedomRisks.pdf.

Musker, R. & Smith, F. (2021). *Incentive Systems for Research Data Sharing in Funded Projects*. Wallingford, United Kingdom: CAB International. https://gatesopenresearch.org/documents/5-84.

Musunuri, S., Sandbrink, J. B., Monrad, J. T., Palmer, M. J., & Koblentz, G. D. (2021). Rapid proliferation of pandemic research: Implications for dual-use risks. *mBio*, *12*(5), e0186421. https://doi.org/10.1128/mBio.01864-21.

NASEM (National Academies of Sciences, Engineering, and Medicine). (2017). *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies*. Washington, D.C.: The National Academies Press. https://doi.org/10.17226/24761.

NASEM (National Academies of Sciences, Engineering, and Medicine). (2022). *Protecting U.S. Technological Advantage*. Washington, D.C.: The National Academies Press. https://doi.org/10.17226/26647.

NASEM (National Academies of Sciences, Engineering, and Medicine). (2024). National Science, Technology, and Security Roundtable-Capstone Workshop. Retrieved November 2024, from https://www.nationalacademies.org/our-work/national-science-technology-and-security-roundtable-capstone-event.

NASEM (National Academies of Sciences, Engineering, and Medicine). (2025). *National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop*. Washington, D.C.: The National Academies Press. https://doi.org/10.17226/27976.

NCSC, CSE, & DHS CISA (National Cyber Security Centre, Communications Security Establishment Canada, and United States' Department of Homeland Security's Cybersecurity and Infrastructure Security Agency). (2020). *Advisory: APT29 Targets COVID-19 Vaccine Development*. London, United Kingdom; Ottawa, ON; Washington, D.C.: NCSC. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf.

NGRAC (Nunatsiavut Government Research Advisory Committee). (n.d.). NGRAC. Retrieved June 2025, from https://nunatsiavut.com/research/ngrac/.

NIAID (National Institute of Allergy and Infectious Diseases). (2021). Pandemic preparedness research approach. Retrieved June 2025, from https://www.niaid.nih.gov/research/pandemic-preparedness-research-approach.

Nicoll, A., Dawson, J., Marty, J., Sawada, M., & Copland, L. (2025). Comparative and critical analysis of data sources used for ship traffic spatial pattern analysis in Canada and across the global Arctic. *Maritime Transport Research*, *8*, 100129. https://doi.org/10.1016/j.martra.2025.100129.

NIH (National Institutes of Health). (2014). *Implementation of the U.S. Government Policy for Institutional Oversight of Life Sciences DURC: Frequently Asked Questions*. Bethesda, MD: NIH.

Nokia Bell Labs. (2022). The transistor: 75 years since the famed Nokia Bell Labs invention changed the world. Retrieved November 2024, from https://www.bell-labs.com/institute/blog/the-transistor-75-years-since-the-famed-nokia-bell-labs-invention-changed-the-world/#gref.

Northrup, S., Lovekin, C., Blais, B., Chartier, R., Davis, R., Mann, P., … Sahrakorpi, S. (2022). *Digital Research Alliance of Canada HPC Strategy*. Toronto, ON: Digital Research Alliance of Canada. https://alliancecan.ca/sites/default/files/2024-03/Digital%20Research%20Alliance%20of%20Canada%20HPC%20Strategy.pdf.

NPSA (National Protective Security Authority). (2023). Five Eyes launches the Five Principles of Secure Innovation. Retrieved November 2024, from https://www.npsa.gov.uk/blog/news/five-eyes-launches-five-principles-secure-innovation.

NPSA & NCSC (National Protective Security Authority and National Cyber Security Centre). (2024). *Trusted Research: Guidance for Academics*. London, United Kingdom: NPSA & NCSC. https://www.npsa.gov.uk/system/files/trusted-research-guidance-for-academia-digital-july24.pdf.

NRC (National Research Council Canada). (2024). Statement on research security. Retrieved May 2025, from https://nrc.canada.ca/en/corporate/values-ethics/statement-research-security.

NSABB (National Science Advisory Board for Biosecurity). (2023). *Proposed Biosecurity Oversight Framework for the Future of Science*. Bethesda, MD: NSABB. https://osp.od.nih.gov/wp-content/uploads/2023/03/NSABB-Final-Report-Proposed-Biosecurity-Oversight-Framework-for-the-Future-of-Science.pdf.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2018). Policy on Intellectual Property. Retrieved June 2025, from http://www.nserc-crsng.gc.ca/NSERC-CRSNG/policies-politiques/ip-pi_eng.asp?utm_source=chatgpt.com.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2023). San Francisco Declaration on Research Assessment (DORA). Retrieved November 2023, from http://www.nserc-crsng.gc.ca/NSERC-CRSNG/policies-politiques/DORA-DORA_eng.asp.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2024a). Research security: Tri-agency guidance on research security. Retrieved April 2024, from https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/index_eng.asp.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2024b). Research security: Tri-agency guidance on the National Security Guidelines for Research Partnerships. Retrieved January 2025, from https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2024c). Alliance Advantage. Retrieved November 2024, from https://www.nserc-crsng.gc.ca/innovate-innover/alliance-alliance/index_eng.asp.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2024d). Research security: Resources. Retrieved November 2024, from https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/resources-ressources_eng.asp.

NSERC (Natural Sciences and Engineering Research Council of Canada). (2025). Research security: Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy). Retrieved June 2025, from https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/strac-rtsap_eng.asp.

NSF (U.S. National Science Foundation). (2023). Dear colleague letter: Workshop to inform development of the NSF Research on Research Security Program (RRSP). Retrieved November 2024, from https://www.nsf.gov/pubs/2023/nsf23126/nsf23126.jsp.

NSF (U.S. National Science Foundation). (2024a). Dear colleague letter: Request for Information on the CHIPS and Science Act Section 10343. Research Ethics. Retrieved November 2024, from https://www.nsf.gov/pubs/2024/nsf24127/nsf24127.jsp.

NSF (U.S. National Science Foundation). (2024b). NSF-backed SECURE Center will support research security, international collaboration. Retrieved October 2024, from https://new.nsf.gov/news/nsf-backed-secure-center-will-support-research.

NSF (U.S. National Science Foundation). (2025). The Research on Research Security Program (RoRS). Retrieved May 2025, from https://www.nsf.gov/funding/opportunities/rors-research-research-security-program.

NSICOP (National Security and Intelligence Committee of Parliamentarians). (2021). *National Security and Intelligence Committee of Parliamentarians Annual Report 2020*. Ottawa, ON: NSICOP. https://nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_en.pdf.

NSTC (National Science and Technology Council). (2022). *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. Washington, D.C.: Subcommittee on Research Security & Joint Committee on the Research Environment. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

OCW (Ministry of Education, Culture and Science). (2023). DBSA 2 published. Retrieved August 2024, from https://english.loketkennisveiligheid.nl/latest/news/2023/01/17/dbsa-2-published.

OCW (Ministry of Education, Culture and Science). (n.d.-a). Contact Point for Knowledge Security. Retrieved August 2024, from https://english.loketkennisveiligheid.nl/.

OCW (Ministry of Education, Culture and Science). (n.d.-b). Legal frameworks and codes of conduct. Retrieved May 2025, from https://english.loketkennisveiligheid.nl/tools-and-frameworks/legal-frameworks-and-codes-of-conduct.

OCW (Ministry of Education, Culture and Science). (n.d.-c). About us: Submit your question to the National Contact Point. Retrieved May 2025, from https://english.loketkennisveiligheid.nl/about-us.

OECD (Organization for Economic Co-operation and Development). (2025). Main science and technology indicators. Retrieved January 2025, from https://www.oecd.org/en/data/datasets/main-science-and-technology-indicators.html.

OFI (Ocean Frontier Institute). (2022). *Indigenous Engagement Guide*. Halifax, NS: OFI. https://www.ofi.ca/impact/indigenous-engagement/guide.

ONC (Ocean Networks Canada). (2021a). *ONC Data Policy*. Victoria, BC: ONC. https://www.oceannetworks.ca/data/data-policy/.

ONC (Ocean Networks Canada). (2021b). Building TRUST to be FAIR: Data stewardship for a sustainable ocean economy. Retrieved December 2024, from https://www.oceannetworks.ca/news-and-stories/stories/building-trust-to-be-fair-data-stewardship-for-a-sustainable-ocean-economy/.

ONC (Ocean Networks Canada). (2023). Decolonizing data. Retrieved January 2025, from https://www.oceannetworks.ca/news-and-stories/stories/decolonizing-data/.

ONC (Ocean Networks Canada). (n.d.-a). Our story. Retrieved June 2024, from https://www.oceannetworks.ca/about-onc/our-story/.

ONC (Ocean Networks Canada). (n.d.-b). Cabled networks. Retrieved November 2024, from https://www.oceannetworks.ca/observatories/physical-infrastructure/cabled-networks.

OPC (Office of the Privacy Commissioner of Canada). (2018). Summary of privacy laws in Canada. Retrieved November 2024, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.

ORCA (Oceans Research in Canada Alliance). (2022). Oceans Research in Canada Alliance. Retrieved June 2024, from https://science.gc.ca/site/science/en/oceans-research-canada-alliance.

ORCA (Oceans Research in Canada Alliance). (2023). *ORCA 2023 National Meeting Summary Report*. St. John's, NL: ORCA. https://science.gc.ca/site/science/en/oceans-research-canada-alliance/orca-2023-national-meeting/orca-2023-national-meeting.

OSTP (White House Office of Science and Technology Policy). (2022). *Desirable Characteristics of Data Repositories for Federally Funded Research*. Washington, D.C.: OSTP. https://repository.si.edu/handle/10088/113528.

OSTP (White House Office of Science and Technology Policy). (2024). *Guidelines for Research Security Programs at Covered Institutions*. Washington, D.C.: OSTP. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf.

OTN (Ocean Tracking Network). (2024). *Ocean Tracking Network Data Policy*. Halifax, NS: OTN. https://members.oceantrack.org/data/policies/.

Owens, B. (2023a, June 14). A new era of research security. *University Affairs*. Retrieved March 2024, from https://universityaffairs.ca/features/feature-article/a-new-era-of-research-security/.

Owens, B. (2023b, April 19). Catching up on open access. *University Affairs*. Retrieved November 2024, from https://universityaffairs.ca/features/feature-article/catching-up-on-open-access/.

Pannier, A. (2023). *Balancing Security and Openness for Critical Technologies: Challenges for French and European Research*. Paris, France: French Institute of International Relations. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_pannier_balancing_security_openness_critical_technologies_2023.pdf.

Paquet, V., Van Bellen, S., & Larivière, V. (2022). Measuring the prevalence of open access in Canada: A national comparison. *The Canadian Journal of Information and Library Science*, *45*(1), 1–21. https://doi.org/10.5206/cjilsrcsib.v45i1.14149.

PHAC (Public Health Agency of Canada). (2015). *Plan for Administrative Oversight for Pathogens and Toxins in a Research Setting: Required Elements and Guidance*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/phac-aspc/documents/services/laboratory-biosafety-biosecurity/licensing-program/plan-administrative-oversight-pathogens-toxins-a-research-setting-required-elements-guidance/admin_oversight-surveillance_admin-eng.pdf.

PHAC (Public Health Agency of Canada). (2018a). *Canadian Biosafety Guideline—Dual-Use in Life Science Research*. Ottawa, ON: Government of Canada. https://www.canada.ca/en/public-health/programs/consultation-biosafety-guideline-dual-use-life-science-research/document.html.

PHAC (Public Health Agency of Canada). (2018b). *Canadian Biosafety Guideline: Conducting a Biosecurity Risk Assessment*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/phac-aspc/documents/services/canadian-biosafety-standards-guidelines/guidance/canadian-biosafety-guidelines/Biosecurity%20RA%20Guide%206May2019.pdf.

PHAC (Public Health Agency of Canada). (2020). *Maximizing Impact: Biosecurity Program Annual Report 2018-2019*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/phac-aspc/documents/services/publications/health-risks-safety/centre-biosecurity-annual-report-2018-2019/phac-biosecurity-annual-report-eng.pdf.

PHAC (Public Health Agency of Canada). (2021). *Scientific Research Policy for Human Pathogens and Toxins*. Ottawa, ON: PHAC. https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/scientific-research-policy-human-pathogens-toxins.html.

PHAC (Public Health Agency of Canada). (2022). *Canadian Biosafety Standard, Third Edition*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/phac-aspc/migration/cbsg-nldcb/cbs-ncb/assets/pdf/canadian-biosafety-standard-third-edition.pdf.

PHAC (Public Health Agency of Canada). (2023). Biosecurity – frequently asked questions. Retrieved June 2025, from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/biosecurity/biosecurity-frequently-asked-questions.html.

PHAC (Public Health Agency of Canada). (2024a). Public Health Agency of Canada Regulatory Compliance and Enforcement Framework. Retrieved May 2025, from https://www.canada.ca/en/public-health/corporate/transparency/regulatory-openness-and-transparency/regulatory-compliance-enforcement-framework.html.

PHAC (Public Health Agency of Canada). (2024b). Frequently asked questions (FAQs): Regulations. Retrieved August 2024, from https://www.canada.ca/en/public-health/corporate/mandate/about-agency/acts-regulations/public-health-agency-canada-interpretation-policy/frequently-asked-questions-faqs-regulations.html.

PHAC (Public Health Agency of Canada). (2024c). Biosecurity. Retrieved January 2025, from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/biosecurity.html.

PHAC (Public Health Agency of Canada). (2024d). Licensing program. Retrieved January 2025, from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/licensing-program.html.

PHAC (Public Health Agency of Canada). (2024e). What we heard: Consultation on potential amendments to the Human Pathogens and Toxins Regulations. Retrieved April 2024, from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/thematic-consultation-human-pathogens-toxins-act-regulations/what-we-heard-consultation-potential-amendments-regulations.html.

PHAC (Public Health Agency of Canada). (2024f). *Biosecurity Addendum to the Canadian Biosafety Standard, Third Edition: For Containment Level 4 Facilities*. Ottawa, ON: Government of Canada. https://training-formation.phac-aspc.gc.ca/pluginfile.php/585259/mod_resource/content/4/Biosecurity%20Addendum%20to%20the%20Canadian%20Biosafety%20Standard%2C%20Third%20Edition.pdf.

PHAC (Public Health Agency of Canada). (2025a). Pathogen safety data sheets. Retrieved June 2024, from https://www.canada.ca/en/public-health/services/laboratory-biosafety-biosecurity/pathogen-safety-data-sheets-risk-assessment.html.

PHAC (Public Health Agency of Canada). (2025b). Publication of the Biosecurity Addendum and updates to the Canadian Biosafety Standard, Third Edition. Retrieved June 2025, from https://training-formation.phac-aspc.gc.ca/mod/page/view.php?id=16605.

Plomp, E., Dintzner, N., Teperek, M., & Dunning, A. (2019). Cultural obstacles to research data management and sharing at TU Delft. *Insights*, 32(29), 1–11. https://doi.org/10.1629/uksg.484.

PMO (Office of the Prime Minister of Canada). (2024a). Securing Canada's AI advantage. Retrieved June 2024, from https://www.pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai.

PMO (Office of the Prime Minister of Canada). (2024b). Joint statement by Prime Minister Trudeau and President von der Leyen on the association of Canada to Horizon Europe. Retrieved November 2024, from https://www.pm.gc.ca/en/news/statements/2024/07/03/joint-statement-prime-minister-trudeau-and-president-von-der-ley.

PMRA (Pest Management Regulatory Agency). (2024). *A Framework for Risk Assessment and Risk Management of Pest Control Products*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/hc-sc/documents/services/consumer-product-safety/reports-publications/pesticides-pest-management/policies-guidelines/risk-management-pest-control-products/GUI-a-framework-for-RA-and-RM-of-PCPs-eng.pdf.

POLAR (Polar Knowledge Canada). (2020). *Polar Knowledge Canada: Strategic Plan*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/polar-polaire/documents/pdf/strategic-plan/strategic-plan-EN.pdf.

POLAR (Polar Knowledge Canada). (2022). *Polar Knowledge: Aqhaliat Report—Volume 4*. Ottawa, ON: Government of Canada. https://www.canada.ca/content/dam/polar-polaire/documents/publications/aqhaliat/volume-4/aqhaliat-volume-4-english.pdf.

POLAR (Polar Knowledge Canada). (2023). Canadian Ranger Ocean Watch (CROW). Retrieved June 2025, from https://www.canada.ca/en/polar-knowledge/publications/aqhaliat/volume-4/infosheets.html.

Polytechnics Canada & BHER (Business + Higher Education Roundtable). (n.d.). *Guide to Research Partnerships with Canada's Colleges & Polytechnics*. Ottawa, ON: Polytechnics Canada & BHER. https://bher.ca/assets-documents/resource/Research-Partnerships-Guide-Colleges-Sept.pdf.

Pouget, H. & Zuhdi, R. (2024, March 5). AI and product safety standards under the EU AI Act. *Carnegie Endowment for International Peace*. Retrieved from https://carnegieendowment.org/research/2024/03/ai-and-product-safety-standards-under-the-eu-ai-act?lang=en.

Prasso, S. (2021, December 14). China Initiative set out to catch spies. It didn't find many. *Bloomberg Businessweek*. Retrieved May 2025, from https://www.bloomberg.com/news/features/2021-12-14/doj-china-initiative-to-catch-spies-prompts-fbi-misconduct-racism-claims.

PS (Public Safety Canada). (2010). *Emergency Management Planning Guide*. Ottawa, ON: Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-pnnng/index-en.aspx#ahral-2-5.

PS (Public Safety Canada). (2012). *All Hazards Risk Assessment Methodology Guidelines 2012-2013*. Ottawa, ON: Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-ll-hzrds-ssssmnt/index-en.aspx.

PS (Public Safety Canada). (2023). Parliamentary committee notes: SRSR committee questions and answers. Retrieved February 2025, from https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240321/04-en.aspx?wbdisable=true.

PS (Public Safety Canada). (2024a). About the Research Security Centre. Retrieved May 2024, from https://www.canada.ca/en/services/defence/researchsecurity/about.html.

PS (Public Safety Canada). (2024b). *National Risk Profile — A National Emergency Preparedness and Awareness Tool*. Ottawa, ON: Government of Canada. https://publications.gc.ca/collections/collection_2024/sp-ps/PS1-27-2024-eng.pdf.

PS (Public Safety Canada). (2024c). Parliamentary committee notes: Immigration security screening—A trilateral program. Retrieved January 2025, from https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20241227/14-en.aspx.

PS (Public Safety Canada). (2024d). Media Lines – Bill C-70, An Act respecting countering foreign interference. Retrieved May 2025, from https://www.justice.gc.ca/eng/trans/bm-mb/other-autre/c70/media-mediatiques.html.

PS (Public Safety Canada). (2024e). Parliamentary committee notes: Research security in Canada. Retrieved November 2024, from https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240813/03-en.aspx.

PSPC (Public Services and Procurement Canada). (2024). Controlled goods: Examining, possessing or transferring. Retrieved July 2024, from https://www.canada.ca/en/public-services-procurement/services/industrial-security/controlled-goods.html.

Rantanen, M., Karpechko, A. Y., Lipponen, A., Nordling, K., Hyvärinen, O., Ruosteenoja, K., … Laaksonen, A. (2022). The Arctic has warmed nearly four times faster than the globe since 1979. *Communications Earth & Environment*, *3*, 168. https://doi.org/10.1038/s43247-022-00498-3.

Rappert, B. & Selgelid, M. J. (Eds.). (2013). *On the Dual Uses of Science and Ethics: Principles, Practices, and Prospects*. Canberra, Australia: ANU E Press.

RBC Thought Leadership. (2024, November 28). Canada's biotech reboot: How to keep the vital life sciences sector strong. Retrieved May 2025, from https://www.rbc.com/en/thought-leadership/the-growth-project/canadas-biotech-reboot-how-to-keep-the-vital-life-sciences-sector-strong/.

RCAT (Research Collaboration Advice Team). (n.d.). About us. Retrieved September 2024, from https://www.gov.uk/government/organisations/research-collaboration-advice-team/about.

RCMP (Royal Canadian Mounted Police). (2024). Hydro-Québec employee charged with espionage. Retrieved June 2025, from https://www.rcmp-grc.gc.ca/en/news/2022/hydro-quebec-employee-charged-espionage?wbdisable=true.

Révelard, A., Tintoré, J., Verron, J., Bahurel, P., Barth, J. A., Belbéoch, M., … Williams, B. (2022). Ocean integration: The needs and challenges of effective coordination within the ocean observing system. *Frontiers in Marine Science*, *8*, 737671. https://doi.org/10.3389/fmars.2021.737671.

Richardson, B. & Hussain, Y. (2022, September 1). Course correction: How international students can help solve Canada's labour crisis. *RBC*. Retrieved February 2025, from https://thoughtleadership.rbc.com/course-correction-how-international-students-can-help-solve-canadas-labour-crisis/.

RIVM (Dutch National Institute for Public Health and the Environment). (n.d.-a). Biosecurity Office. Retrieved August 2024, from https://www.bureaubiosecurity.nl/en.

RIVM (Dutch National Institute for Public Health and the Environment). (n.d.-b). Dual-use animation. Retrieved August 2024, from https://www.bureaubiosecurity.nl/en/dual-use-animatie.

RIVM (Dutch National Institute for Public Health and the Environment). (n.d.-c). Dual-Use Quickscan. Retrieved May 2024, from https://dualusequickscan.com/en/.

Robinson, J. (2020). *Arctic Space Challenge for NATO Emerging from China's Economic and Financial Assertiveness*. Kalkar, Germany: Joint Air Power Competence Centre. https://www.japcc.org/articles/arctic-space-challenge-for-nato-emerging-from-chinas-economic-and-financial-assertiveness/.

Rohden, F. & Wieden, H.-J. (2022). Introduction: Dual use in life science research. *Biochemistry and Cell Biology*, *100*, 266–267. https://doi.org/10.1139/bcb-2022-0082.

Rubinstein, Y. R., Robinson, P. N., Gahl, W. A., Avillach, P., Baynam, G., Cederroth, H., … Haendel, M. A. (2020). The case for open science: Rare diseases. *JAMIA Open*, *3*(3), 472–486. https://doi.org/10.1093/jamiaopen/ooaa030.

Sandbrink, J. B. & Koblentz, G. D. (2022). Biosecurity risks associated with vaccine platform technologies. *Vaccine*, *40*, 2514–2523. https://doi.org/10.1016/j.vaccine.2021.02.023.

Science-Metrix. (2024). *Bibliometric Analysis for the Expert Panel on the State of Science, Technology, and Innovation in Canada*. Montréal, QC: Shared online by the CCA. https://cca-reports.ca/wp-content/uploads/2025/11/science-metrix-bibliometric-analysis-for-the-expert-panel-on-the-state-of-science-technology-and-innovation-in-canada-2025.pdf.

SECD (Standing Senate Committee on National Security, Defence and Veterans Affairs). (2023). *Arctic Security under Threat: Urgent Needs in a Changing Geopolitical and Environmental Landscape*. Ottawa, ON: SECD. https://sencanada.ca/content/sen/committee/441/SECD/reports/2023-06-28_SECD_ArcticReport_e.pdf.

SFU (Simon Fraser University). (2023). SFU Open Access Policy. Retrieved November 2024, from https://www.lib.sfu.ca/help/publish/scholarly-publishing/open-access/open-access-policy.

SGDSN (General Secretariat for National Defence and Security). (2018). *Protection numerique du potentiel scientifique et technique de la nation*. Paris, France: SGDSN. https://www.sgdsn.gouv.fr/files/files/Nos_missions/guide_protection_scientifique_technique_nation_anssi-pa-049_v1.pdf.

SGDSN (General Secretariat for National Defence and Security). (n.d.). *La protection du potentiel scientifique et technique de la nation*. Paris, France: SGDSN. https://www.sgdsn.gouv.fr/files/files/Nos_missions/a5-ppst-v5.pdf.

Shankar, A. & Drake, W. (2022). *Effective Cybersecurity for Research*. Bloomington, IN: Center for Applied Cybersecurity Research, Indiana University. https://library.educause.edu/-/media/files/library/2022/6/researchcybersecurity.pdf.

Sharma, Y. (2025, April 17). Academics say draft screening law could deter foreign talent. *University World News*. Retrieved June 2025, from https://www.universityworldnews.com/post.php?story=20250417132055569.

Shea, D. A. (2006). *Balancing Scientific Publications and National Security Concerns: Issues for Congress*. Washington, D.C.: U.S. Congressional Research Service. https://sgp.fas.org/crs/secrecy/RL31695.pdf.

SIGRE (Security and Integrity of the Global Research Ecosystem Working Group). (2022). *G7 Common Values and Principles on Research Security and Research Integrity*. n.l.: SIGRE. https://science.gc.ca/site/science/sites/default/files/attachments/2023/1135-g7-common-values-and-principles-on-research-security-and-research-integrity_.pdf.

SIGRE (Security and Integrity of the Global Research Ecosystem Working Group). (2024). *G7 Best Practices For Secure & Open Research*. n.l.: SIGRE. https://science.gc.ca/site/science/sites/default/files/documents/1136-g7-best-practices-for-secure-and-open-research-february-2024.pdf.

Silbey, S. S. (2022). Why do biologists and chemists do safety differently? The reproduction of cultural variation through pragmatic regulation. In N. Gross, I.A. Reed, & C. Winship (Eds.), *The New Pragmatist Sociology: Inquiry, Agency, and Democracy* (1st ed.). New York, NY: Columbia University Press.

Simard, M.-A., Ghiasi, G., Mongeon, P., & Larivière, V. (2022). National differences in dissemination and use of open access literature. *PLOS ONE*, *17*(8), e0272730. https://doi.org/10.1371/journal.pone.0272730.

Smith, G. C., Allard, R., Babin, M., Bertino, L., Chevallier, M., Corlett, G., … the WWRP PPP Steering Group. (2019). Polar ocean observations: A critical gap in the observing system and its effect on environmental predictions from hours to a season. *Frontiers in Marine Science*, *6*, 429. https://doi.org/10.3389/fmars.2019.00429.

Snipp, C. M. (2016). What does data sovereignty imply: What does it look like? In T. Kukutai & J. Taylor (Eds.), *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australia: Australian National University Press.

Spitale, G., Germani, F., & Biller-Andorno, N. (2024). Disruptive technologies and open science: How open should open science be? A 'third bioethics' ethical framework. *Science and Engineering Ethics*, *30*, 36. https://doi.org/10.1007/s11948-024-00502-3.

SRO (Safeguarding Research Office). (2024a). *Understanding and Adhering to Government of Ontario Research Security Requirements*. Edmonton, AB: Office of the Vice-President (Research & Innovation), University of Alberta.

SRO (Safeguarding Research Office). (2024b). *2024 Impact Report*. Edmonton, AB: Office of the Vice-President (Research & Innovation), University of Alberta. https://www.ualberta.ca/en/research/media-library/services/2024-safeguarding-research-office-impact-report.pdf.

SRO (Safeguarding Research Office). (2025). *Responsible Open Source Due Diligence Protocol*. Edmonton, AB: Office of the Vice-President (Research & Innovation), University of Alberta. https://www.ualberta.ca/en/research/media-library/services/responsible-open-source-due-diligence-protocol.pdf.

SRSR (Standing Committee on Science and Research). (2024). *The Security of Research Partnerships between Canadian Universities, Research Institutions and Entities Connected to the People's Republic of China*. Ottawa, ON: House of Commons. https://publications.gc.ca/collections/collection_2024/parl/xc79-1/XC79-1-1-441-10-eng.pdf.

StatCan (Statistics Canada). (2020). Estimation of research and development expenditures in the higher education sector. Retrieved June 2025, from https://www.statcan.gc.ca/en/statistical-programs/document/5109_D3_T9_V1.

StatCan (Statistics Canada). (2023). Table 37-10-0020-01: Postsecondary graduates, by institution type, status of student in Canada and gender. Retrieved November 2024, from https://www150.statcan.gc.ca/t1/tbl1/en/cv.action?pid=3710002001.

StatCan (Statistics Canada). (2024a). Table 27-10-0273-01 (formerly CANSIM 358-0001): Gross domestic expenditures on research and development, by science type and by funder and performer sector (x 1,000,000). Retrieved June 2025, from https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2710027301.

StatCan (Statistics Canada). (2024b). Table 37-10-0135-01: Postsecondary graduates, by field of study, International Standard Classification of education, age group and gender. Retrieved June 2025, from https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3710013501.

StatCan (Statistics Canada). (2024c). Table 36-10-0604-01: Activities of multinational enterprises in Canada, Canadian and foreign multinationals, by sector and industry. Retrieved September 2024, from https://www150.statcan.gc.ca/t1/tbl1/en/cv.action?pid=3610060401.

StatCan (Statistics Canada). (2024d). Statistics Canada Open Science Action Plan. Retrieved November 2024, from https://www.statcan.gc.ca/en/about/osap.

Stirling, A., Hayes, K. R., & Delborne, J. (2018). Towards inclusive social appraisal: Risk, participation and democracy in governance of synthetic biology. *BMC Proceedings*, *12*(Suppl 8), 15. https://doi.org/10/gr5fcp.

Sun, K., Cui, W., & Chen, C. (2021). Review of underwater sensing technologies and applications. *Sensors*, *21*, 7849. https://doi.org/10.3390/s21237849.

Tatlow, D. K. (2024, July 21). China's expanding Arctic ambitions challenge the U.S. and NATO. *Newsweek*. Retrieved August 2024, from https://www.newsweek.com/2024/08/09/china-russia-us-arctic-north-pole-strategy-svalbard-norway-sea-route-1916641.html.

Tayler, F., Moher, D., & Cobey, K. (2020). Creating an Audit and Feedback Loop to Monitor and Enhance Data Sharing in Canada. *University of Ottawa. Preprint*. https://ruor.uottawa.ca/handle/10393/41562.

TBS (Treasury Board of Canada). (2014). *Directive on Open Government*. Ottawa, ON: Government of Canada. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=28108.

TBS (Treasury Board of Canada). (2018). Canada's 2018-2020 National Action Plan on Open Government. Retrieved November 2024, from http://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government.

The Alliance (Digital Research Alliance of Canada). (2021). *Researcher Needs Assessment: Summary of What We Heard*. Toronto, ON: The Alliance. https://alliancecan.ca/sites/default/files/2022-03/needsassessment_alliance_20220126.pdf.

The Alliance (Digital Research Alliance of Canada). (2024). *2024 Resource Allocations Competition Results*. Toronto, ON: The Alliance. https://alliancecan.ca/en/2024-resource-allocations-competition-results.

The Australia Group. (2023). Control list of dual-use biological equipment and related technology and software. Retrieved May 2024, from https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/dual_biological.html.

Thomson, J. (2017, August 2). Canadian military developing surveillance system to monitor Arctic waters. *CBC News*. Retrieved November 2024, from https://www.cbc.ca/news/canada/north/cause-array-drdc-test-1.4232348.

Tiku, N. & de Vynck, G. (2023, May 4). Google shared AI knowledge with the world—until ChatGPT caught up. *The Washington Post*. Retrieved June 2025, from https://www.washingtonpost.com/technology/2023/05/04/google-ai-stop-sharing-research/.

TIPS (Tri-Agency Institutional Programs Secretariat). (2022). Research security. Retrieved October 2024, from https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-eng.aspx.

TIPS (Tri-Agency Institutional Programs Secretariat). (2024). Research security funding for 2023–24. Retrieved October 2024, from https://www.rsf-fsr.gc.ca/apply-demande/grants-subventions/rs2023-eng.aspx.

TOH (The Ottawa Hospital). (2021, March 17). Patient gets life-changing diagnosis thanks to open science. *The Ottawa Hospital*. Retrieved November 2024, from https://www.ottawahospital.on.ca/en/healthy-tomorrows/patient-gets-life-changing-diagnosis-thanks-to-open-science/.

Trevena, P. (2019). *Post Study Work Visa Options: An International Comparative Review.* Edinburgh, United Kingdom: Government of Scotland. https://dera.ioe.ac.uk/id/eprint/33953/1/post-study-work-visa-options-international-comparative-review.pdf.

TRIUMF. (2018). *TRIUMF Strategic Plan 2020–2025*. Vancouver, BC: TRIUMF. https://fiveyearplan.triumf.ca/wp-content/uploads/2019/05/TRIUMF-Strategic-Plan-Web-Pages.pdf.

TU Delft (Delft University of Technology). (n.d.). Data stewardship. Retrieved November 2024, from https://www.tudelft.nl/en/library/research-data-management/r/support/data-stewardship.

U of A (University of Alberta). (2024a). *Research Security Requirements At-a-Glance Tool*. Edmonton, AB: Safeguarding Research Office. https://www.ualberta.ca/en/research/media-library/services/updated-october-2024-research-security-at-a-glance-tool.pdf.

U of A (University of Alberta). (2024b). *Safeguarding Research: Research Security Overview Presentation*. Edmonton, AB: Safeguarding Research Office.

U of A (University of Alberta). (2025). Safeguarding your research. Retrieved March 2025, from https://www.ualberta.ca/en/research/services/safeguarding-your-research.html.

U of T (University of Toronto). (2022). *Canada's AI Ecosystem: Government Investment Propels Private Sector Growth*. Toronto, ON: U of T. https://gro.utoronto.ca/wp-content/uploads/2022/04/Canadas__AI__Ecosystem-__Government__Investment__Propels__Private__Sector__Growth.pdf.

U of T (University of Toronto). (2025). Report Number 215 of the Planning & Budget Committee. Retrieved June 2025, from https://governingcouncil.utoronto.ca/secretariat/page/governance-bodies/planning-and-budget-committee/reports/feb-12-2025.

U of T (University of Toronto). (n.d.). Research security: Safeguarding research. Retrieved March 2025, from https://research.utoronto.ca/safeguarding-research/research-security-safeguarding-research.

U15 (U15 Group of Canadian Researcher Universities). (2023). *Safeguarding Research in Canada: A Guide for University Policies and Practices*. n.l.: U15. https://u15.ca/wp-content/uploads/2023/06/2023-06-22.-U15-Leading-Practices-Safeguarding-Research-FINAL-3.pdf.

U15 & Universities Canada (U15 Group of Canadian Researcher Universities). (2019a). *Travel Security Guide for University Researchers and Staff*. Ottawa, ON: U15 and Universities Canada. https://univcan.ca/wp-content/uploads/2020/08/travel-security-guide-for-university-researchers-and-staff-dec-2019.pdf.

U15 & Universities Canada (U15 Group of Canadian Researcher Universities). (2019b). *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects—A Tool for University Researchers*. Toronto, ON: U15 and Universities Canada. https://www.univcan.ca/wp-content/uploads/2020/08/mitigating-economic-and-or-geopolitical-risks-in-sensitive-research-projects-dec-2019.pdf.

UCalgary & U of A (University of Calgary and University of Alberta). (2023). *Research Security Conference Summary: Mitigating Risk in a Changing World*. Calgary, AB: UCalgary & U of A. https://www.ualberta.ca/en/research/media-library/services/2023-rs-conference-summary-notes.pdf.

UCalgary (University of Calgary). (2025). Alberta Research Security Community of Practice Workshop/AGM. Retrieved May 2025, from https://events.ucalgary.ca/event/494400-alberta-research-security-community-of-practice.

Ueno, H. (2023). Artificial intelligence as dual-use technology. In I.K. Hatzilygeroudis, G.A. Tsihrintzis, & L.C. Jain (Eds.), *Fusion of Machine Learning Paradigms: Theory and Applications*. Cham, Switzerland: Springer.

UFIT (University Foreign Interference Taskforce). (2021). *Guidelines to Counter Foreign Interference in the Australian University Sector*. Canberra, Australia: Government of Australia. https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector.

Uhlenhaut, C., Burger, R., & Schaade, L. (2013). Protecting society: Biological security and dual-use dilemma in the life sciences—status quo and options for the future. *EMBO Reports*, *14*(1), 25–30. https://doi.org/10.1038/embor.2012.195.

UKRI (United Kingdom Research and Innovation). (2024a). Ensuring open research. Retrieved August 2024, from https://www.ukri.org/what-we-do/supporting-healthy-research-and-innovation-culture/open-research/.

UKRI (United Kingdom Research and Innovation). (2024b). Trusted research and innovation. Retrieved August 2024, from https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/.

UN (United Nations). (2007). *United Nations Declaration on the Rights of Indigenous Peoples*. New York, NY: UN. https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf.

UNESCO (United Nations Educational, Scientific and Cultural Organization). (2021). *UNESCO Recommendation on Open Science*. Paris, France: UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000379949.

UNGA (The United Nations General Assembly). (1948). *Universal Declaration of Human Rights*. New York, NY: UNGA. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

UNGA (United Nations General Assembly). (1966). *International Covenant on Economic, Social and Cultural Rights*. New York, NY: UNGA. https://www.ohchr.org/sites/default/files/cescr.pdf.

Universities Australia. (2024). *Legislative review of the Australia's Foreign Relations (State and Territory Arrangements) Act 2020*. Deakin, Australia: Universities Australia. https://universitiesaustralia.edu.au/wp-content/uploads/2024/08/Submission-to-the-review-of-Australias-Foreign-Relations-State-and-Territory-Arrangements-Act-2020.pdf.

Universities Canada. (2024). *Briefing Note on New Research Security Measures*. Ottawa, ON: Universities Canada. https://www.ulethbridge.ca/sites/default/files/2024/02/universities_canada_-_research_security_goc_announcement_briefing_note_to_member_insititutions.pdf.

Universities UK, CPNI, & UKRI (Centre for the Protection of National Infrastructure and UK Research and Innovation). (2022). *Managing Risks in International Research and Innovation: An Overview of Higher Education Sector Guidance*. London, United Kingdom: Universities UK, CPNI, & UKRI. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf.

University of Cambridge. (n.d.). Data champions. Retrieved November 2024, from https://www.data.cam.ac.uk/intro-data-champions.

University of Tokyo. (n.d.). U.S.–Canada–Japan International Workshop on Research Security and Integrity. Retrieved May 2025, from https://ifi.u-tokyo.ac.jp/en/event/13105/.

UNL (Universities of the Netherlands). (2024). *Capability Maturity Model: Knowledge Security*. The Hague, the Netherlands: UNL. https://www.universiteitenvannederland.nl/files/publications/UNL%20Capability%20Maturity%20Model%20Knowledge%20Security%20ENG-DEF.pdf.

UNZ (Universities New Zealand – Te Pōkai Tara). (2022). *Trusted Research – Protective Security Requirements: Guide for Senior University Leaders in Aotearoa New Zealand*. Wellington, New Zealand: UNZ. https://www.universitiesnz.ac.nz/sites/default/files/uni-nz/Main%20guide_as%20single%20pages.pdf.

uOttawa (University of Ottawa). (2022). *Policy 128: International Travel Safety Policy*. Ottawa, ON: uOttawa. https://www.uottawa.ca/about-us/leadership-governance/policies-regulations/policy-128-international-travel-safety-policy.

U.S. GAO (U. S. Government Accountability Office). (2022). National security space: Actions needed to better use commercial satellite imagery and analytics. Retrieved June 2025, from https://www.gao.gov/products/gao-22-106106.

UVic (University of Victoria). (2024). Implication of Ontario research security guidelines. Retrieved February 2025, from https://www.uvic.ca/research-services/funding/research-security/announcements/ontario-research-security.php.

UVic (University of Victoria). (2025). Research security. Retrieved March 2025, from https://www.uvic.ca/research-services/funding/research-security/index.php.

van der Molen, I., Gheorghe, D., Daouti, C., & Eechaudt, V. (2023). *Keeping Science Open? Current Challenges in the Day-to-Day Reality of Universities*. Leuven, Belgium: Conference of European Schools for Advanced Engineering Education and Research (CESAER). https://zenodo.org/doi/10.5281/zenodo.8355324.

Verga, S. (2013). *A Holistic, Cross-Government All Hazards Risk Assessment*. Ottawa, ON: Defence Research and Development Canada, Centre for Security Science. https://publications.gc.ca/collections/collection_2017/rddc-drdc/D69-26-2013-eng.pdf.

VIDO (Vaccine and Infectious Disease Organization). (2025). Community Liaison Committee. Retrieved March 2025, from https://www.vido.org/about/community-liaison-committee.php.

VIDO (Vaccine and Infectious Disease Organization). (n.d.). Facilities. Retrieved January 2025, from https://www.vido.org/about/facilities.php.

VU Amsterdam (Vrije Universiteit Amsterdam). (2023). Sleuteltechnologieën [Key technologies]. Retrieved August 2024, from https://assets-us-01.kc-usercontent.com/d8b6f1f5-816c-005b-1dc1-e363dd7ce9a5/2db06628-bbe9-43cb-8ee9-8064899405ca/Sleuteltechnologie%C3%ABn%20-%20Key%20technology%202023.pdf.

Wagner, W. J. & Zaia, R. (2023, November 17). The intersection between national security research guidelines and export/import laws in Canada: What institutions should know. *Gowling WLG*. Retrieved June 2024, from https://gowlingwlg.com/en/insights-resources/articles/2023/national-security-research-guidelines/.

Wang, L.-F., Lewin, S. R., Zhong, N., Zhang, L., Chen, Z., Yuen, K.-Y., & Ho, D. D. (2025). Pandemic research: The need for a paradigm shift. *The Lancet Microbe*, *6*. https://doi.org/10.1016/j.lanmic.2024.101048.

WAS (Wassenaar Arrangement Secretariat). (2023). *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. Vienna, Austria: WAS. https://www.wto.org/english/res_e/booksp_e/int_exp_regs_part3_5_e.pdf.

Weisko, P. (2025, March 25). Dragon on ice: China's geostrategic interests in the Arctic. *Institute for National Security Studies, Tel Aviv University*. Retrieved May 2025, from https://www.inss.org.il/publication/north-pole/.

Whalen, D., Forbes, D. L., Kostylev, V., Lim, M., Fraser, P., Nedimović, M. R., & Stuckey, S. (2022). Mechanisms, volumetric assessment, and prognosis for rapid coastal erosion of Tuktoyaktuk Island, an important natural barrier for the harbour and community. *Canadian Journal of Earth Sciences*, *59*, 945-960. https://doi.org/10.1139/cjes-2021-0101.

WHO (World Health Organization). (2022). *Global Guidance Framework for the Responsible Use of the Life Sciences: Mitigating Biorisks and Governing Dual-Use Research*. Geneva, Switzerland: WHO. https://iris.who.int/bitstream/handle/10665/362313/9789240056107-eng.pdf?sequence=1.

WHOI (Woods Hole Oceanographic Institution). (n.d.). Areas of research. Retrieved June 2025, from https://www.whoi.edu/what-we-do/understand/areas-of-research/.

Wilner, A., Beach-Vaive, S., Carbonneau, C., Hopkins, G., & Leblanc, F. (2022). Research at risk: Global challenges, international perspectives, and Canadian solutions. *International Journal*, 77(1), 26-50. https://doi.org/10.1177/00207020221118504.

WIPO (World Intellectual Property Organization). (n.d.). WIPO Guide to Trade Secrets and Innovation—Part II: Strategic roles of trade secrets in the innovation ecosystem. Retrieved November 2024, from https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-ii-strategic-roles-of-trade-secrets-in-the-innovation-ecosystem.html.

Wölfl, A.-C., Snaith, H., Amirebrahimi, S., Devey, C. W., Dorschel, B., Ferrini, V., … Wigley, R. (2019). Seafloor mapping—The challenge of a truly global ocean bathymetry. *Frontiers in Marine Science*, *6*, 283. https://doi.org/10.3389/fmars.2019.00283.

Woods, H. B. & Pinfield, S. (2022). Incentivising research data sharing: A scoping review. *Wellcome Open Research*, *6*, 355. https://doi.org/10.12688/wellcomeopenres.17286.2.

Yao, D. (2023, May 8). Google to halt sharing AI research—Until product is developed. *AI Business*. Retrieved November 2024, from https://aibusiness.com/companies/google-to-halt-sharing-ai-research-until-product-is-developed.

Yoshizawa, G., Shinomiya, N., Kawamoto, S., Kawahara, N., Kiga, D., Hanaki, K.-I., & Minari, J. (2023). Limiting open science? Three approaches to bottom-up governance of dual-use research of concern. *Pathogens and Global Health*. https://doi.org/10.1080/20477724.2023.2265626.

Zandee, D., Kruijver, K., & Stoetman, A. (2020). *The Future of Arctic Security: The Geopolitical Pressure Cooker and the Consequences for the Netherlands*. The Hague, the Netherlands: The Netherlands Institute of International Relations (Clingendael). https://www.clingendael.org/sites/default/files/2020-04/Report_The_Future_of_Arctic_Security_April_2020.pdf.

Zhang, F. (2019). Development of CRISPR-Cas systems for genome editing and beyond. *Quarterly Reviews of Biophysics*, *52*(e6), 1–31. https://doi.org/10.1017/S0033583519000052.

Zheng, E. (2021, October 28). Choosing open: How to find an open access route that works for you. University of Alberta Library News. Retrieved June 2025, from https://news.library.ualberta.ca/blog/tag/scholarly-comms-and-open/.

# CCA Board of Directors*

**Soheil Asgarpour, FCAE, (Chair),** Past-President, Petroleum Technology Alliance Canada; Past President, Canadian Academy of Engineering (Vancouver, BC)

**Brian Fleck,** Professor, Faculty of Engineering, Mechanical Engineering Department, University of Alberta (Edmonton, AB)

**Pascal Grenier,** Senior Vice President, Flight Services and Global Operations, CAE (Montréal, QC)

**Jawahar (Jay) Kalra, MD, (FCAHS), (Vice-Chair),** Professor, Department of Pathology and Laboratory Medicine and Member, Board of Governors, University of Saskatchewan (Saskatoon, SK)

**Catherine Karakatsanis, FCAE,** Chief Operating Officer, Stantec (formerly Morrison Hershfield Group) Inc.; President, Canadian Academy of Engineering (Toronto, ON)

**Catherine Middleton,** Professor, Ted Rogers School of Information Technology Management, Toronto Metropolitan University (Toronto, ON)

**Hasna Rouighi,** Director, Office of Innovation, Ministry of Health and Social Services, Government of Québec (Montréal, QC)

**Donna Strickland, C.C., FRSC, FCAE,** Professor, Department of Physics and Astronomy, University of Waterloo (Waterloo, ON)

**Christine Thomas,** Vice-President, Governance and Legal Counsel, Canadian Medical Association (Ottawa, ON)

**Gisèle Yasmeen,** Global Fellow, Wilson Center (Ottawa, ON)

*As of July 2025

# CCA Scientific Advisory Committee*

**Maydianne C. B. Andrade (Chair),** Professor, Biological Sciences, University of Toronto Scarborough; President, Canadian Black Scientists Network (Toronto, ON)

**Peter Backx, FRSC, FCAHS,** Professor, Department of Biology, and Canada Research Chair in in Cardiovascular Biology, York University (Toronto, ON)

**Kyle Bobiwash,** Assistant Professor and Indigenous Scholar, Department of Entomology, University of Manitoba (Winnipeg, MB)

**Bing Chen,** Professor of Civil Engineering, UArctic Chair in Marine and Coastal Environmental Engineering, and Associate Dean of the Faculty of Engineering & Applied Science, Memorial University of Newfoundland (St. John's, NL)

**Benoît Dupont,** Professor, School of Criminology, Canada Research Chair in Cybersecurity, University Research Chair in the Prevention of Cybercrime, Université de Montréal; Scientific Director, Human-Centric Cybersecurity Partnership (Montréal, QC)

**Jaigris Hodson,** Canada Research Chair (Tier 2), Digital Communication for the Public Interest and Associate Professor, College of Interdisciplinary Studies, Royal Roads University (Victoria, BC)

**Digvir S. Jayas. O.C., FRSC, FCAE,** President and Vice-chancellor, University of Lethbridge (Lethbridge, AB)

**Catherine L. Mah,** Professor and Canada Research Chair in Promoting Healthy Populations, School of Health Administration, Faculty of Health, Healthy Populations Institute, Dalhousie University (Halifax, NS)

**Louise Poissant, FRSC,** Scientific Director of Fonds de recherche du Québec – Société et culture (Montréal, QC)

**Nicole Redvers,** Associate Professor and Western Research Chair, Schulich School of Medicine & Dentistry, Western University; VP Research, Association of Faculties of Medicine of Canada (London, ON)

**Madison Rilling,** Executive Director, Optonique (Québec, QC)

**David A. Wolfe,** Professor Emeritus and Co-Director of the Innovation Policy Lab, Munk School of Global Affairs and Public Policy, University of Toronto (Toronto, ON)

*As of July 2025

Evidence for the public good.

The **Council of Canadian Academies (CCA)** is a trusted voice at the intersection of research, society, and public policy, convening expertise and assessing knowledge to advance evidence-informed decision-making in Canada and internationally.

Through expert-led multidisciplinary assessments that draw on evidence from across sectors and communities, the CCA brings clarity, rigour, and balance to understanding the evidence on complex policy topics in diverse areas including health, the environment, public safety, innovation, and the economy.

As a not-for-profit charitable organization, the CCA is guided by the principles of independence, excellence, and integrity in all of its work, delivering consistent value to those using CCA reports to inform policy and public debate.

www.cca-reports.ca

Council of Canadian Academies | Conseil des académies canadiennes