Research Security and Ethics

Parallel Session

Research Security and Ethics

Marlies Rise

Assistant VP, Research Services, Dalhousie University, Canada

Research Security

Presented by Dr. Marlies Rise
Assistant Vice-President,
Research Services

DALHOUSIE UNIVERSITY

Acknowledgements

Dalhousie University is located in Mi’kma’ki, the ancestral and unceded territory of the Mi’kmaq. We are all Treaty people.

We recognize that African Nova Scotians are a distinct people whose histories, legacies and contributions have enriched that part of Mi’kma’ki known as Nova Scotia for over 400 years.

Research Security:
A Changing Landscape

Canadian Context

On July 12, 2021, the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry; the Honourable Bill Blair, Minister of Public Safety and Emergency Preparedness; and the Honourable Patty Hajdu, Minister of Health introduced the National Security Guidelines for Research Partnerships.

- integrates national security considerations into the development, evaluation, and funding of research partnerships.

Home

Français

UA AU University Affairs Affaires universitaires

News Opinion Features Career Advice Subscribe Magazine Search Jobs

A new era of research security

National security agencies are taking a renewed interest in universities and their research in the face of rising geopolitical concerns.

BY BRIAN OWENS
JUN 14 2023

Federal agencies and research funders had been touting the value of international research collaboration for years. When they started to publicly question the safety of such partnerships, the change in tone seemed abrupt, says Dr. Carvin. It's left many researchers unsure of how to navigate this new reality. "For the past two or three decades, academics have been told to go out and get as much international funding and partnerships as we can, and now we're suddenly told to hit the brakes," she says. "There is a palpable sense of whiplash."

RESEARCH SECURITY RISKS – Guidance from Government of Canada

- https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/what-are-risks

  (Nov 2021)

  - Unwanted access and potential interference
  - Theft of research data
  - Loss of intellectual property, patent opportunities, and potential revenue
  - Legal or administrative reprisal
  - Loss of potential future partnerships
  - Tarnished reputation

RESEARCH SECURITY – The changing landscape of higher ed research

Since COVID (2020) the higher education sector has seen a significant shift in both the focus and effectiveness of threat actors

i. Cyber attacks are increasing at a minimum of 50% year-over-year; and Education and Research were measured in 2021 as the most attacked sectors
   - ❑ Check Point Research: Cyber Attacks Increased 50% Year over Year - Check Point Blog

ii. There are professional threat actors who primarily target the education sector
   - ❑ Universities and colleges cope silently with ransomware attacks | CSO Online

iii. Threat actor groups were responsible for 200+ major data theft/ransomware incidents in the US alone, in 2022.
   - ❑ Ransomware Hit 200 US Gov, Education and Healthcare Organizations in 2022 - SecurityWeek

iv. The education sector is regularly rated as one of the least effective sectors in managing cybersecurity risk
   - ❑ 10 Concerning Stats About Cybersecurity in Higher Ed | Collegis Education

This threat actor trend has accelerated in 2023, and the minimum costs - per incident - are currently $3-5 million

RESEARCH SECURITY – Early Intersections in Canadian Research Admin

- Impacts on university research: US Federal Agencies amended the Federal Acquisition Regulation (FAR) to implement Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232). https://www.acquisition.gov/Section-889-Policies
  - Prohibits executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system…unless an exception applies or a waiver is granted.
  - The statute covers certain telecommunications equipment and services produced or provided by ***listed entities***.
  - Required an integrated approach in address (e.g. ORS, ITS, Financial Services, Procurement, Legal, etc.) to enable representation in US System for Award Management (SAM)
- Universities developed and shared best practices (e.g. control frameworks, methods to assess equipment, regular communication of requirements, etc.)

Canadian Developments

- To ensure the Canadian research ecosystem is as open as possible and as safeguarded as necessary, the Government of Canada introduced the National Security Guidelines for Research Partnerships to integrate national security considerations into the development, evaluation and funding of research partnerships.
- Rollout in the NSERC Alliance Program; new programs periodically
- Presented a Risk Assessment Form (RAF) "…to identify and assess potential risks that research partnerships may pose to Canada's national security as outlined in the National Security Guidelines for Research Partnerships and to develop effective mitigation measures."

Risk Assessment Form - Section 1 “Know Your Research”

- Questions include: -
  - Are you working in a research area that is related to:

  1) critical minerals, including critical mineral supply chains

  2) a research area that is classified within one of the critical infrastructure sectors of the National Strategy for Critical Infrastructure (e.g. Energy and utilities, Water, Finance, Safety, Food, Manufacturing, Transportation, Information and communication technology, Government, Health)

  3) the use of personal data that could be sensitive

  4) the development or use of large datasets that could be sensitive

  5) goods or technology that are included on the Export Control List (ECL) of the Export and Import Permits Act (EIPA)

  6) Research areas that may be considered sensitive or dual-use as listed in List 1 of Annex A of the National Security Guidelines for Research Partnerships (*Note: list may be updated periodically in accordance with the evolution of technologies, the military and intelligence applications of technology, and national security imperatives*)

Risk Assessment Form - Section 2 “Know Your Partner Organization”

- The purpose of this section is to assess whether your partner organization(s) could pose a national security risk by using the research knowledge, technology and intellectual property resulting from the research project.
- From the RAF: “Answer the following questions to the best of your ability by using information that is already available to you, your institution, or your partner organization(s), or ***that could be reasonably accessed through open sources***. To further support transparency and openness, you are encouraged to consult your partner organization(s) when answering these questions.”
- Questions include:
  - Are there any indications that your partner organization(s) could be subject to foreign government influence, interference or control?
  - Are there any indications that suggest a lack of transparency or unethical behaviour from your partner organization(s), that may impact the proposed research project?
  - Are there any indications that an individual(s) involved in the research project from your partner organization(s) could have conflicts of interest or affiliations that could lead to unauthorized knowledge transfer?
  - Are there any indications that as a result of this research project, your partner organization(s) will or could have access to your research institution’s Canadian facilities, networks, or assets on campus, including infrastructure that houses sensitive data?

The list will include foreign-state-connected universities, research institutes and laboratories that are believed to be at "higher risk" of engaging in theft, unwanted knowledge transfers and interference in research, according to government documents reviewed by the Star.

Risk Assessment Form - Section 4 “Risk Mitigation Plan”

- The risk mitigation plan ensures that you identify the appropriate mitigation measures to reduce the likelihood of an identified security risk materializing, and/or to lessen the impact in case the identified risk materializes.
- Additional information on risk mitigation can be found on the Safeguarding Your Research portal (https://science.gc.ca/site/science/en/safeguardingyour-research)
  - Guidelines and Tools to Implement Research Security (March 2023)
    - Mitigating Your Research Security Risks – training, DMP, Cyber security, agreement on research finding use, etc.

Risk Assessment Form - Section 5 “Additional Requirements”

- “By submitting this Risk Assessment Form, the applicant on behalf of all co-applicants agrees that, to the best of their knowledge:

  - The applicant(s) have not accepted and will not accept any offer of funding that is conditional upon the mirroring of their academic laboratory in, or the transfer of their academic laboratory to, a foreign country; and
  - The source of funding and the value of the research project to the partner organization(s) has been communicated by the partner organization(s) to the applicant(s).”

National Security Guidelines for Research Partnerships: Guiding Principles

- "The Government of Canada recognizes that Canada's research ecosystem needs to be as open as possible and as safeguarded as necessary so it benefits Canada, Canadians, and the global good. The federal government and stakeholders in the research enterprise have a shared responsibility to protect the integrity of the research ecosystem and safeguard it from activities that undermine the foundational principles of openness, transparency, merit, and reciprocity that underlie the research ecosystem in Canada."

  - **Academic Freedom**
  - **Institutional Autonomy**
  - **Freedom of Expression**
  - **Equity, Diversity, and Inclusion**
    - Freedom from discrimination is a fundamental and internationally recognized human right that is necessary for all aspects of the research enterprise.
  - **Research in the Public Interest**
  - **Transparency**
  - **Integrity**
  - **Collaboration**

https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships

Budget 2022 proposed to **implement the National Security Guidelines for Research Partnerships fully**, with $159.6 million starting in 2022-23, and $33.4 million ongoing

$125 million over five years, starting in 2022-23, and $25 million ongoing, for the Research Support Fund to build capacity within postsecondary institutions to identify, assess, and mitigate potential risks to research security; and

$34.6 million over five years, starting in 2022-23, and $8.4 million ongoing, to enhance Canada's ability to protect its research, and to establish a Research Security Centre that will provide advice and guidance directly to research institutions.

Best Practices:
In development

RESEARCH SECURITY – Safeguarding Research at Canada's Universities

- Universities are developing and sharing best practices to uphold global engagement, critical to competitiveness on the world stage, while safeguarding research from the potential risks in global research engagement
  - Upholding EDIA
  - Governance and Risk Frameworks
  - Strategic planning
  - Government engagement
  - Communication, Education and Knowledge Sharing
  - Network and Device Security
  - Innovation – Fit for Purpose Solutions

SecureScholar.ca

A web application to help institutions evaluate research projects based on the risks identified in the *National Security Guidelines for Research Partnerships'* Risk Assessment Form.

Works by data mining millions of public records from a variety of sources.

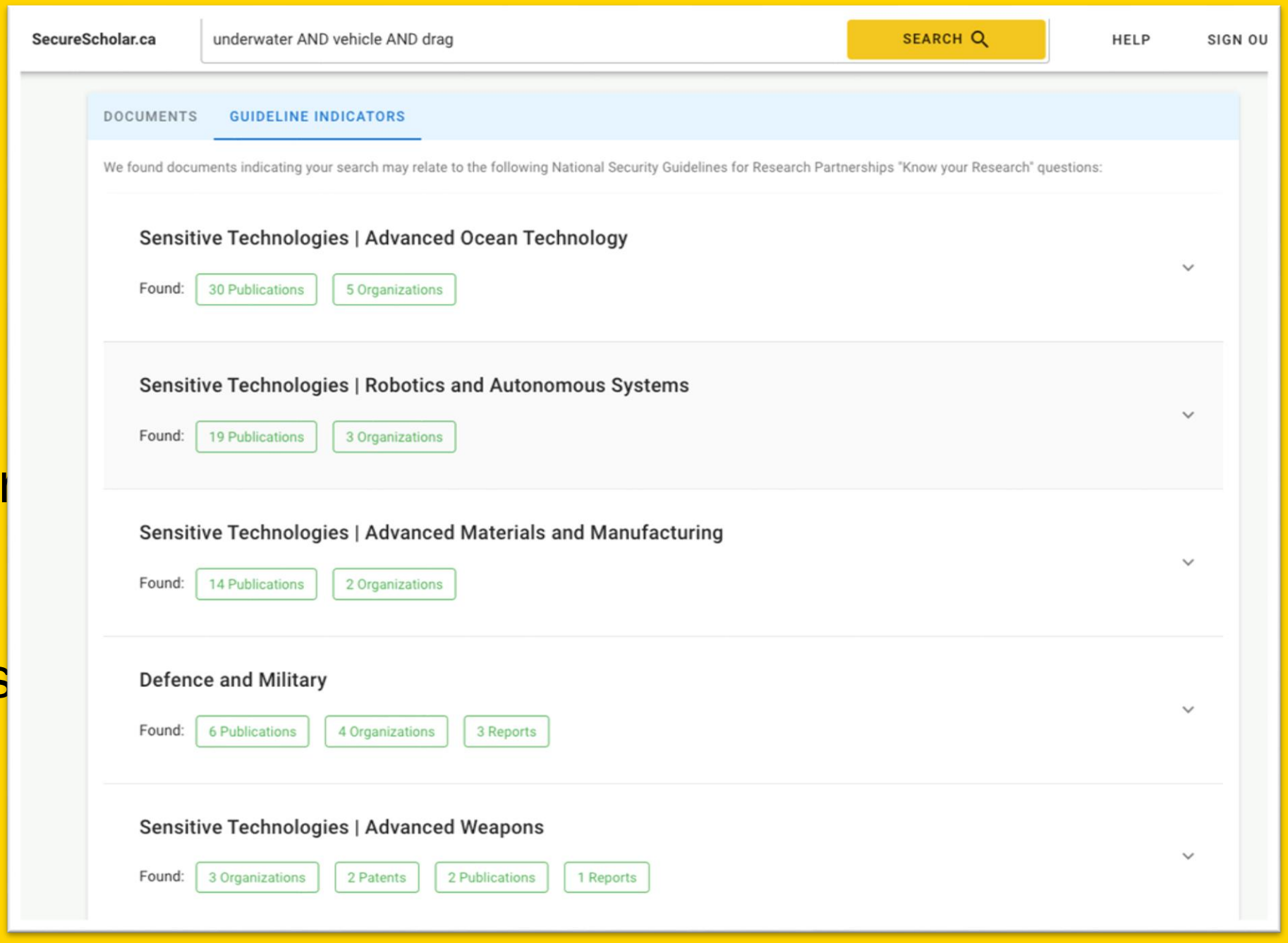
Created by the U15, but being made available as a private Beta to U15 and non-U15 institutions.

Actively being developed with a focus on building features based on institutional feedback.

U15 Canada

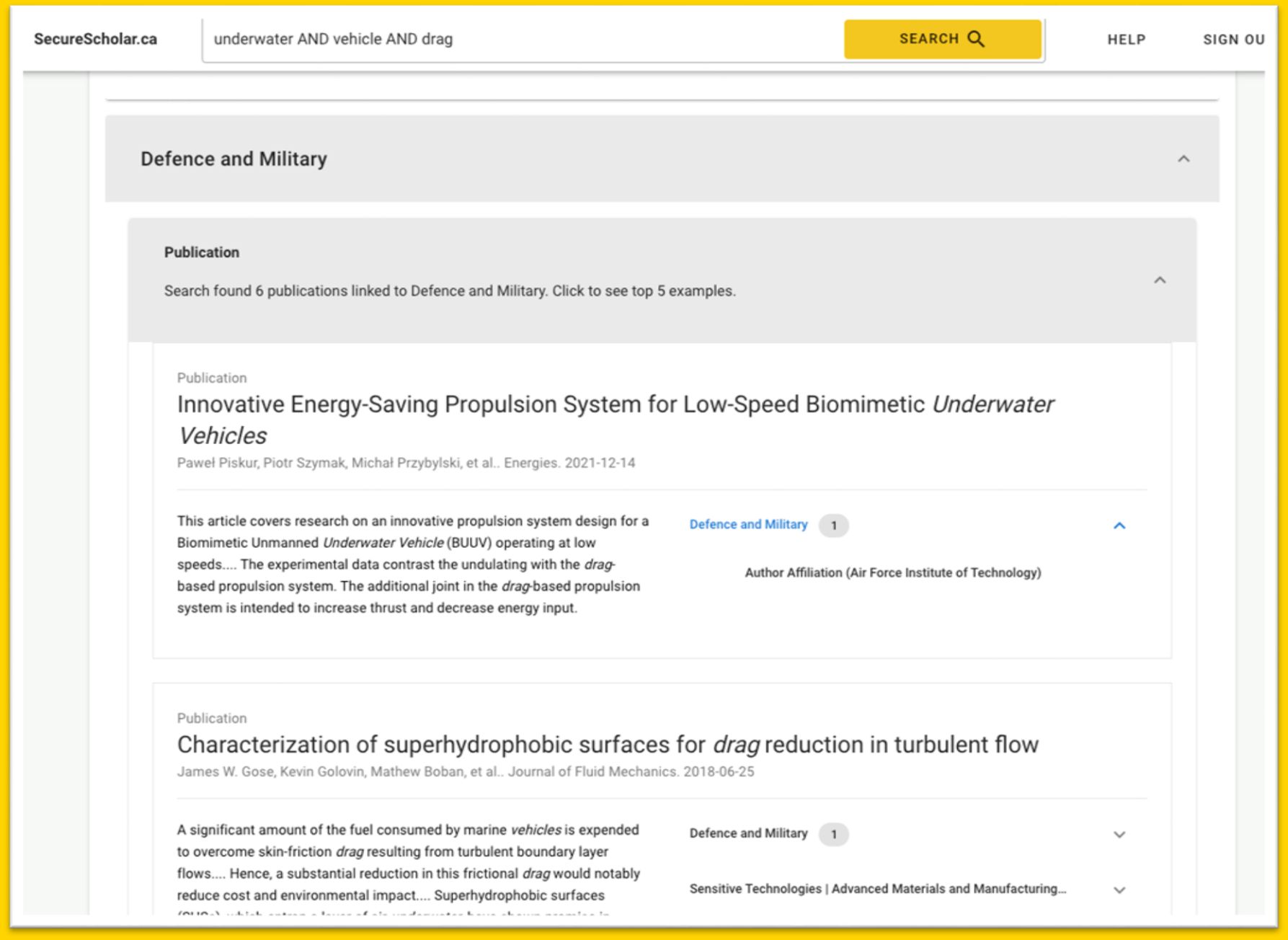
Mike Matheson
Managing Director (Cognit.ca) /
Directeur principal (Cognit.ca)
360, rue Albert Street, Suite 1425, Ottawa, ON K1R 7X7

Quickly see how research topics relate to Know Your Research Risks in the National Security Guidelines for Research Security.



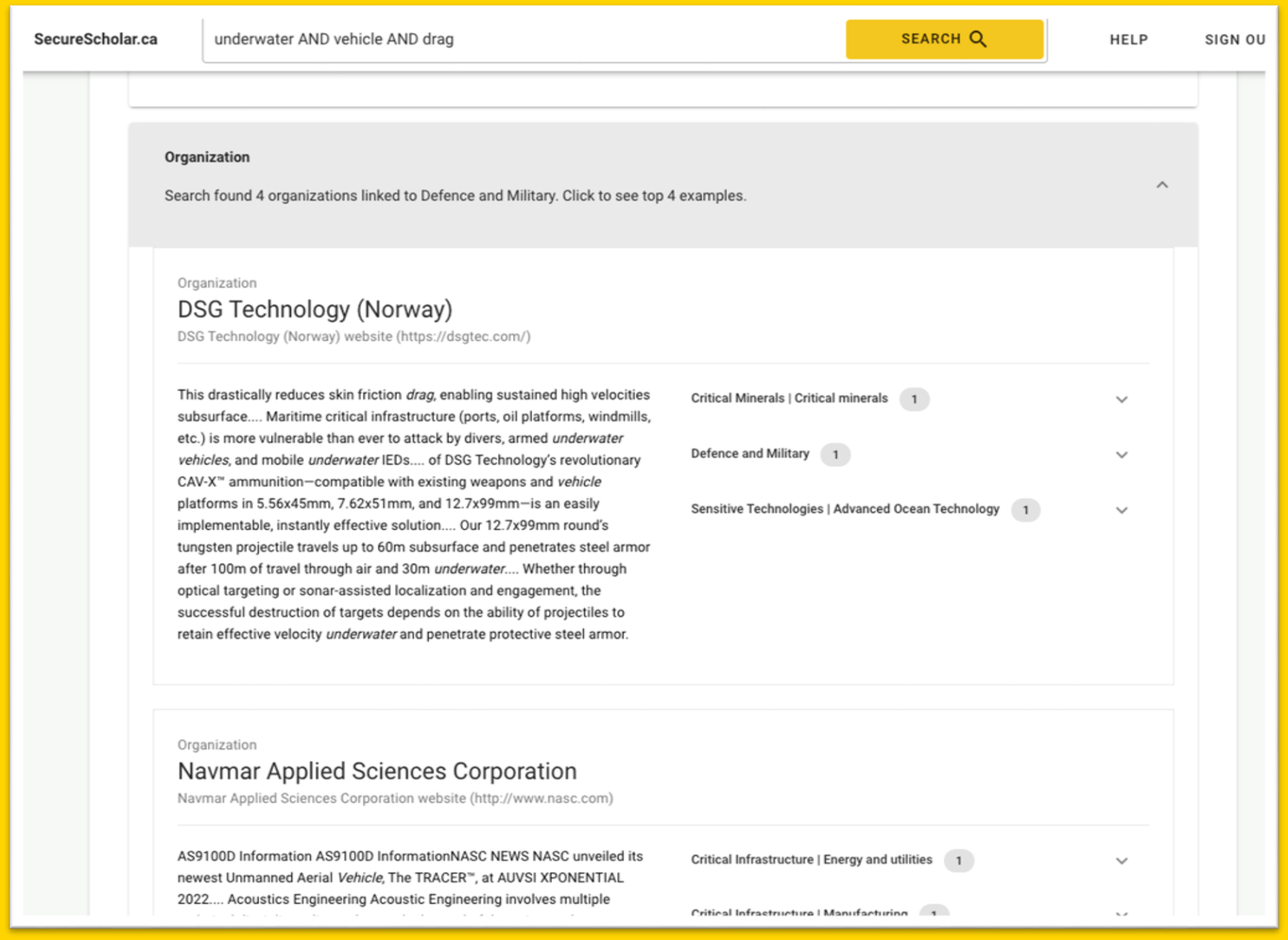
Contributed by Mike Matheson

Understand why a topic relates to a given research security consideration.



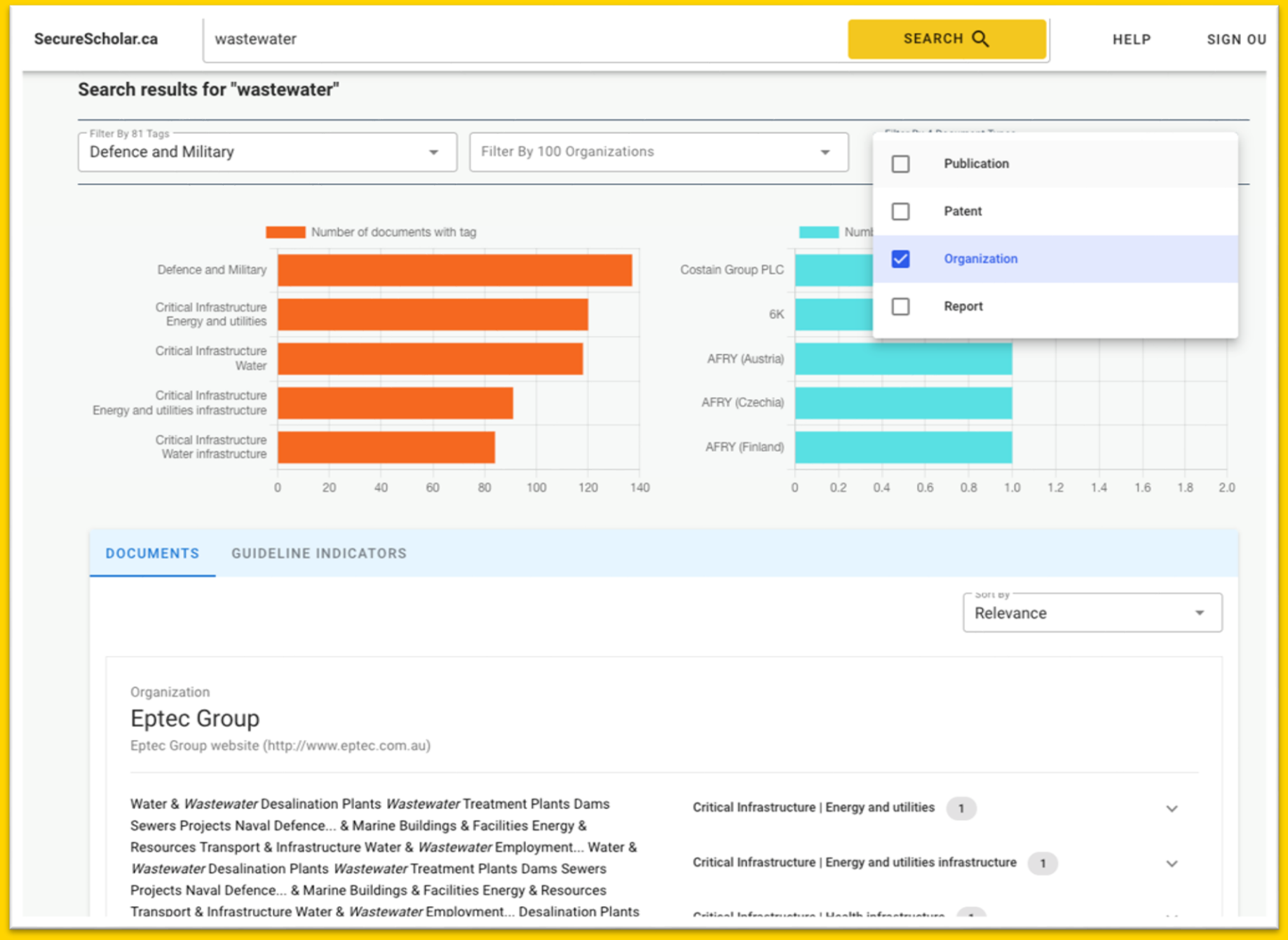
Contributed by Mike Matheson

Find organizations that are interested in the topic.



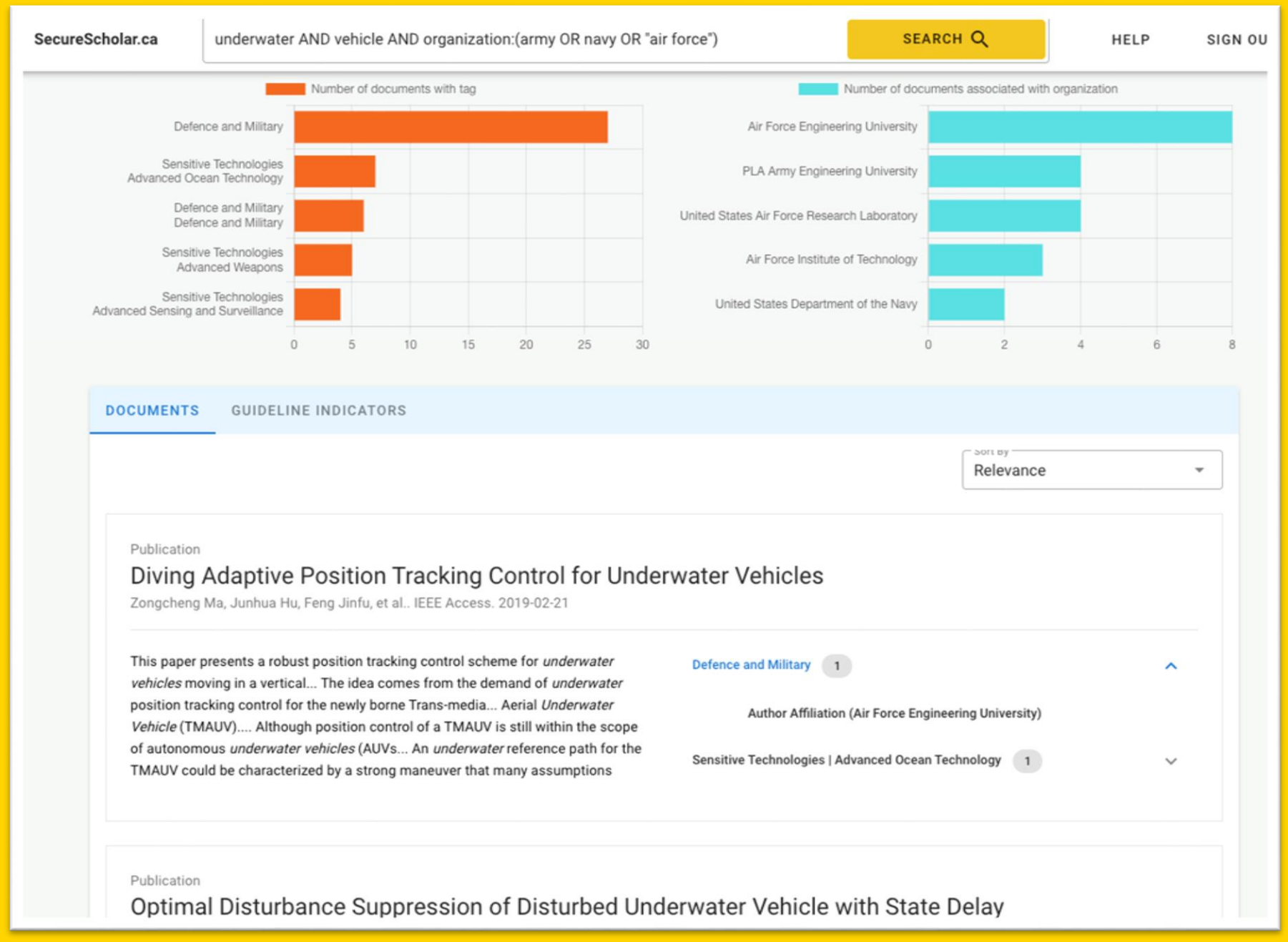
Contributed by Mike Matheson

Pinpoint the results you care about using filters.



Contributed by Mike Matheson

Answer arbitrary questions using advanced searches.



Contributed by Mike Matheson

SecureScholar.ca – Beta Test Observations

SecureScholar.ca outputs specifically map to the security risk assessment forms required for (NSERC, +++) grant application submission, and are particularly useful in supporting researchers in considering connections between their areas of research and research areas that are sensitive or dual-use.

Upcoming developments are anticipated to significantly simplify due diligence in assessing partner organization(s) and their relevant affiliates.

This innovation will greatly enhance capacity for research security assessment, and enable broad support for researchers toward better understanding how their research aligns with sensitive areas, as well as enable researchers to more readily identify partner connections needing attention or risk mitigation toward promoting research security.

Other Commercial Solutions

Kharon - risk data and software solutions powering compliance, risk management, investigations, and analytic operations. (https://www.kharon.com/#kharon-company)

Strider - Intelligence Platform is a data as a service (DaaS) platform to deliver strategic intelligence specifically designed to visualize, manage, and respond to risks. (https://www.striderintel.com/)

Questions?

Parallel Session

Research Security and Ethics

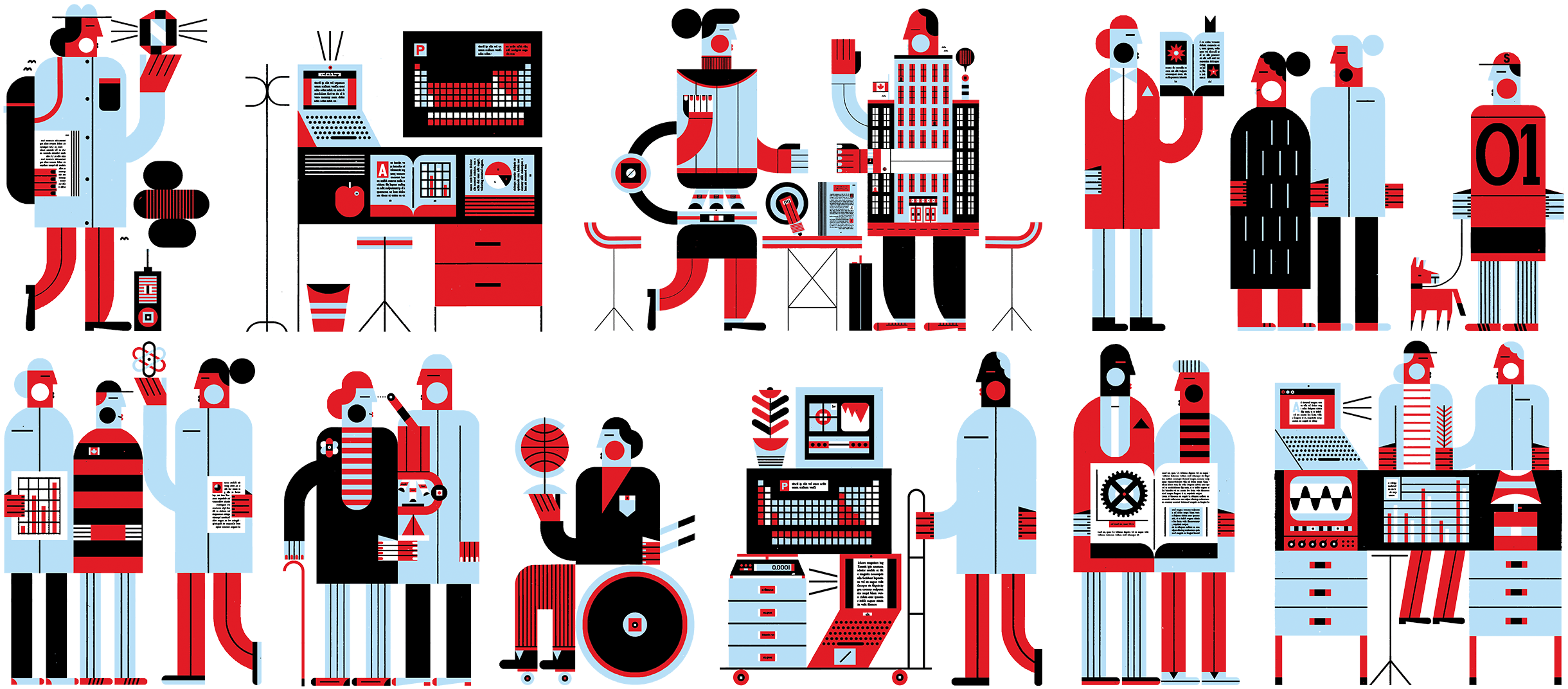
Shawn McGuirk

Deputy Director, Natural Sciences and Engineering Research Council, Canada

NSERC
CRSNG

Breakthrough answers
to timeless questions

Des réponses innovantes
à de grandes questions



Natural Sciences and Engineering
Research Council of Canada

Conseil de recherches en sciences
naturelles et en génie du Canada

Canada

Research Security

NSERC & the Government of Canada

Shawn McGuirk

Deputy Director, Research Security – NSERC

What is Research Security?

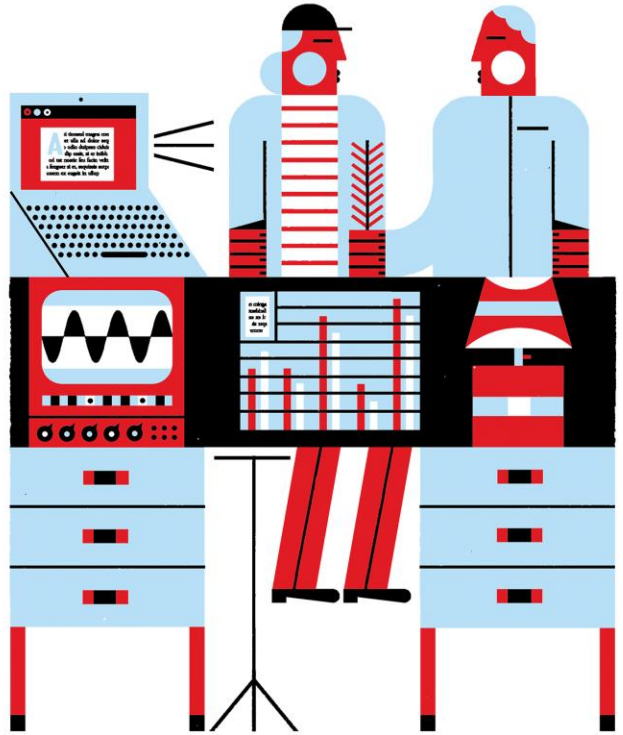
G7 Common Values and Principles on Research Security and Research Integrity

- Maintaining openness to a maximum extent, with ethical & security safeguards
- Balancing national and global interests
- Accountability and responsibility for due diligence, research management, and research impacts
- Shared responsibilities between all members of the research community
- Collaboration and dialogue with all members of the research community
- Proactive efforts to address risks
- Adaptability to changing risks
- Proportionality between risk & response

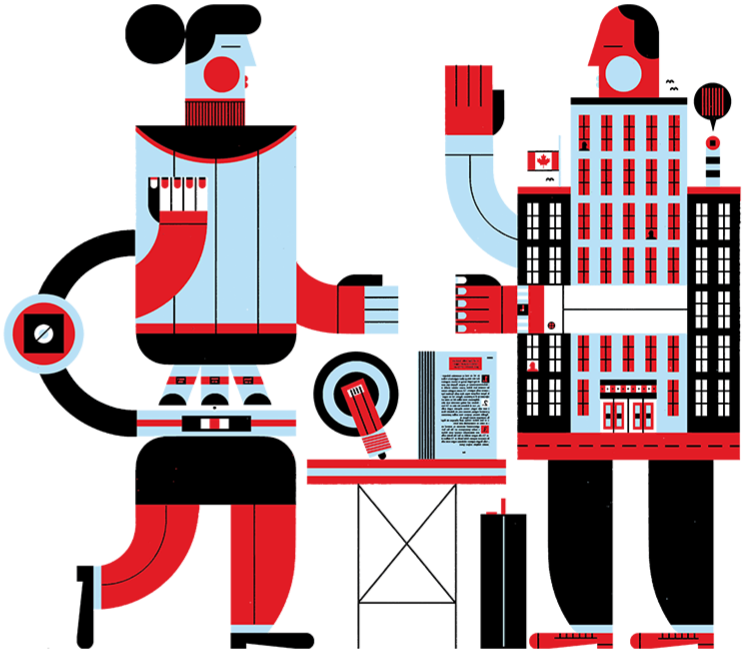
What is Research Security?

- Research security actions **protect the integrity of research**, with emphasis on **protecting against threats to national and economic security**. This includes actions that protect against the theft and misappropriation of research, the unauthorized transfer of ideas, research outcomes, and intellectual property.
- As a set of activities, research security encompasses:
  - The **identification of possible risks** to research by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and
  - The activities that **protect research** inputs and processes, research outcomes, and intellectual property (including sensitive research and personal data) from **interference & misappropriation**.
- Identifying and mitigating risks often results in positive impacts, by protecting and promoting research integrity and trust. Appropriate and risk-targeted measures can enhance the foundations of academic freedom, research integrity, open science, transparency, and trusted collaborations for mutual benefit
- Disproportionate research security measures can lead to restrictions on scientific and academic freedom and openness (e.g., discouraging fruitful and positive collaborations). In worst cases, this can lead to **racial profiling** and may also **erode the benefits of international collaboration**. .

Table of contents



Canada's approach to research security



Research security & the granting agencies – timeline

- **2018 –** The Government of Canada (GoC)–Universities Working Group is created to share information on and coordinate actions to address foreign interference in Canadian research.
- **2020 –** The GoC-Universities Working Group publishes the *Safeguarding Your Research* portal; Ministerial statement tasks the federal granting agencies (NSERC, SSHRC, CIHR) and the CFI to review their policies to better integrate national security considerations into their activities.
- **Spring 2021 –** Ministerial statement tasks the GoC–Universities Working Group to develop the *National Security Guidelines for Research Partnerships* (the NSGRP), in 90 days.
- **Summer 2021 –** Ministers release the NSGRP and apply them immediately as a pilot to NSERC's Alliance grants program, for applications with private sector partner organizations.
- **Spring 2022 –** Federal budget invests in further implementation of the NSGRP, in a federal Research Security Centre, and in support for research-intensive universities via the Research Support Fund.
- **Summer 2022 –** Publication of the G7 Statement of Principles on Research Security and Integrity.
- **Spring 2023 –** Update to the *Agreement on the Administration of Agency Grants and Awards by Research Institutions*; New ministerial statement requests new policy measures .

Key Principles

Canada's research ecosystem needs to be as **open as possible** and as **secure as necessary**, so that it benefits Canada, Canadians, and the global good.

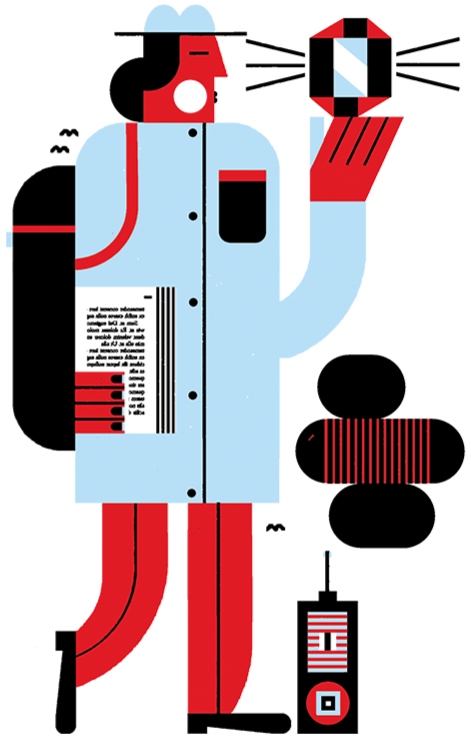
The Government of Canada, granting agencies, and research community have a **shared responsibility** to:

- Protect the integrity of our research ecosystem and to safeguard it from activities that undermine its principles of openness, transparency, merit, academic freedom, and reciprocity; and,
- Ensure that research security measures (new and existing) do not lead to discrimination against or profiling of any member of the community.

Dialogue and collaboration between all parties in the research ecosystem is critical, so that we can adopt shared approaches and ensure that research security measures are:

- Clear and consistent;
- Well understood and implementable by researchers and institutions;
- Proportionate to the level of risk; and
- Balanced with existing, shared commitments (e.g., to open science and EDI)

Safeguarding Science & Safeguarding Your Research



Safeguarding Science

Promoting Awareness of Chemical, Biological, Radiological, and Nuclear Security Risks, and the Potential Proliferation of Dual-use Technology

[Research Security Training Courses]

[Case Studies - Scenarios]

[Guidance on Conducting Open Source Due Diligence]

[Guidance for Research Organizations and Funders]

The *National Security Guidelines for Research Partnerships*

About the National Security Guidelines for Research Partnerships

The National Security Guidelines for Research Partnerships ("the Guidelines") were developed via the Government of Canada-Universities Working Group, to integrate national security considerations into the development, evaluation, and funding of research partnerships.

They Guidelines were established following a set of guiding principles:

- ✓ Academic Freedom
- ✓ Institutional Autonomy
- ✓ Freedom of Expression
- ✓ Transparency
- ✓ Integrity
- ✓ Collaboration
- ✓ Equity, Diversity, and Inclusion
- ✓ Research in the Public Interest

The Guidelines recognize that:

- Canada's research ecosystem needs to be as **open as possible** and as **secure as necessary**, so that it benefits Canada, Canadians, and the global good.
- The federal government and stakeholders across Canada's research ecosystem have a **shared responsibility** to protect the integrity of this ecosystem and safeguard it from activities that undermine its foundational principles of openness, transparency, merit, and reciprocity.

National Security Guidelines for Research Partnerships

Table of Contents

Innovation, Science and Economic Development Canada | Innovation, Sciences et Développement économique Canada

Protected When Completed

National Security Guidelines for Research Partnerships Risk Assessment Form

Save As | Print | Reset

Family name of applicant:	Initial(s) of all given names of applicant:	Grant administering institution:

Introduction

The Risk Assessment Form is a tool to identify and assess potential risks that research partnerships may pose to Canada's national security as outlined in the National Security Guidelines for Research Partnerships and to develop effective mitigation measures.

In answering the Risk Assessment Form questions, you will provide information – to the best of your ability – that is specific to your proposed area of research and prospective research partner organizations. This information will be used to assess national security risks where the proposed research partnership could expose the research project to foreign interference, espionage or theft from foreign governments, militaries and other organizations, and also pose potential risks to the wider Canadian research enterprise.

For the purpose of the National Security Guidelines for Research Partnerships, a partner organization is any organization that plays an active role in the project and/or supports a research partnership through cash and/or in-kind contributions. Examples of a partner organization's role may include:

- Sharing in intellectual leadership or providing expertise;
- Active participation in research activities; and/or
- Application of research results and/or active participation in translating or mobilizing the knowledge produced to help achieve the desired outcomes of the project.

National security risks may be described as, but not limited to circumstances where there are potential instances of foreign interference, espionage, intellectual property theft or unauthorized knowledge transfer that:

- contribute to the advancement of military, security, and intelligence capabilities of states or groups that pose a threat to Canada; and/or
- disrupt the development of Canadian research and innovation, weaken the resiliency of critical infrastructure, or jeopardize the protection of sensitive data of Canadians.

The information collected will not be used to substantiate if you are compliant with any legislative or regulatory requirements that may apply to your proposed research project. The collection of this information will be used to assess the overall risk profile of your research project.

Who needs to complete the Risk Assessment Form?

Anyone can use the Risk Assessment Form to conduct due diligence when establishing and/or continuing partnerships with national, international and multinational partners.

This form may be required for specified federal research funding opportunities. You should consult the appropriate program literature associated with the funding opportunity to which you are applying to determine if you are required to submit a Risk Assessment Form with your grant application.

Depending on the specific funding opportunity, the "applicant" may be an individual, on behalf of any co-applicants, or may be a post-secondary or research institution.

What resources and tools may assist you?

You are encouraged to conduct open-source research to complete the Risk Assessment Form and to consult with your partner organization(s), where appropriate, to validate the information. For more information, consult the comprehensive guide Conducting Open Source Due Diligence for Safeguarding Research Partnerships.

Section 1: Know Your Research

The purpose of this section is to gather key information about your research. This information will be used to assess whether the nature and/or usability of your **research project** could attract the interest of foreign governments, militaries, their proxies, and other organizations who may seek to exploit research partnerships to access research information, research knowledge, and the resulting intellectual property and technology to facilitate unauthorized knowledge transfer.

Research areas that are sensitive or dual-use, in that they have military, intelligence, or dual military/civilian applications, are more likely to present national security risks.

Answers to the following questions will assist in determining the overall risk profile of your research project. Risk Assessment Forms are assessed on a case-by-case basis, and answering "yes" or "unsure" to any of these questions is not a determinant of a denial of funding. For more information on the risk assessment process, consult the Safeguarding Your Research portal.

Section 2: Know Your Partner Organization

The purpose of this section is to assess whether **your partner organization(s)** could pose a national security risk by using the research knowledge, technology and intellectual property resulting from your research project. Your research can be an attractive target for those seeking to steal, use, and adapt it for their own priorities and gains. In some instances, research could lead to advancements in the strategic, military, or intelligence capabilities of other countries or be used to purposefully cause harm to Canada's national security.

The following questions serve as a source of information to assist in determining the overall risk profile of your research partnership. Answering "yes" or "unsure" to any of these questions is not a determinant of a denial of funding.

Answer the following questions to the best of your ability by using information that is already available to you, your institution, or your partner organization(s), or that could be reasonably accessed through open sources. To further support transparency and openness, you are encouraged to consult your partner organization(s) when answering these questions. The Government of Canada may request more information from your partner organization(s) for the purposes of national security risk assessment.

When answering these questions, you must consider and include information not only about your partner organization(s) but also their relevant affiliates. Therefore, for the purpose of this section, the term 'partner organization' also includes any affiliated parent organizations, subsidiaries, and joint ventures in Canada and abroad.

Section 3: Risk Identification

The purpose of this section is to collect information on any **risk factors** that you have **identified** in the two first sections of the form. To support the risk assessment process, your response must provide information on the source and nature of the risks.

For each "**yes**" or "**unsure**" response that you provided in the Know Your Research **and** Know Your Partner Organization sections, describe the **resources** you utilized and the **key findings** you gathered.

You may add any other relevant or contextual information related to your partner organization(s) in this section. For example, list any concerns noted during your due diligence process that have not been captured in a previous section of this form.

Section 4: Risk Mitigation Plan

The purpose of this section is to present your **risk mitigation plan**. This plan will ensure that you identify the appropriate mitigation measures to reduce the likelihood of an identified security risk materializing, and/or to lessen the impact in case the identified risk materializes.

When developing your risk mitigation plan, you must address all risk factors that you identified by answering "**yes**" or "**unsure**" to questions in the Know Your Research **and** Know Your Partner Organization sections.

Your risk mitigation plan should be developed **with your institution**. You may also involve your institution's corporate support services (e.g., IT, security, legal) to confirm the viability and feasibility of the proposed measures.

Mitigation measures should be tailored to the research project and commensurate with the risks identified while considering open science principles. For instance, your risk mitigation plan could cover areas, such as, but not limited to:

- Describing any other relevant review processes for which the project has been subject to (e.g., a Research Ethics Board review focusing on how personal data gathered through the research project will be safeguarded)
- Raising research security awareness and building capacity across your research team
- Ensuring that your partner organization(s)' objectives align with the objectives of the partnership
- Ensuring sound cybersecurity and data management practices
- Agreement on the intended use of research findings

For each mitigation measure you propose, you must also provide a **timeline** for its implementation and describe **how you and your institution will monitor its effectiveness**.

It is not sufficient to refer to existing or upcoming policies and practices within your institution. If you refer to a policy or practice, you must also describe **what** this policy or practice entails and **how** it will be applied to mitigate the identified risks.

The National Security Guidelines for Research Partnerships are country and company-agnostic as risks can evolve and originate from anyone and anywhere in the world. Following the principles of the Guidelines, risk mitigation measures must never lead to discrimination against or profiling of a member of the research community. Accordingly, excluding any individual from participating in the proposed research project on the basis of their citizenship or country of residence is **not** an acceptable risk mitigation measure.

Section 5: Additional Requirements

By submitting this Risk Assessment Form, the applicant on behalf of all co-applicants agrees that, to the best of their knowledge:

- The applicant(s) have not accepted and will not accept any offer of funding that is conditional upon the mirroring of their academic laboratory in, or the transfer of their academic laboratory to, a foreign country; and
- The source of funding and the value of the research project to the partner organization(s) has been communicated by the partner organization(s) to the applicant(s).

Implementation of the NSGRP in NSERC's Alliance grants program

- Since July 23, 2021, Alliance applications with a private sector partner organization must be submitted with a completed Risk Assessment Form.
- NSERC's dedicated **Research Security Team** reviews the Risk Assessment Form as part of the administrative process, prior to merit review. This process includes **ensuring completeness of the form** as well as an **administrative risk validation** using open-source intelligence (OSINT) methods.
- Any application with possible or identified risks is referred to NSERC's Risk Assessment Committee. The majority of applications are cleared by NSERC at this level.
- Where necessary (~4% of cases), NSERC requests **national security risk assessment and advice.** These are cases where:
  - the nature of the proposed research could be deemed sensitive (Annex A) and
  - the private sector partner organizations were identified from open-source information to be:
    - associated with, or originating from, countries/organizations under sanctions, and/or
    - associated with criminal or ethical concerns.

Implementation of the NSGRP in NSERC's Alliance grants program

- On request by NSERC, Canada's national security departments and agencies assess the risks associated with the research partnership, consider the proposed mitigations, and provide advice to **inform NSERC's funding decision.**
- NSERC makes its funding decision by considering the results of the merit review and, where applicable, the national security advice received.
- If a research partnership proposal is assessed to present an unacceptable risk to Canada's national security and/or where risks cannot be appropriately mitigated, research funding will be declined.
- When NSERC notifies applicants of its funding decision:
  - NSERC communicates new/relevant information from security agencies in the decision letter
  - Applicants are offered the opportunity to request a meeting (with NSERC & Public Safety)
  - In all cases, NSERC points applicants to resources on the Safeguarding Your Research portal

Impact of the NSGRP on NSERC's Alliance grants program

NSERC analyzed data from the pilot in Alliance (July 2021 – July 2022). As of March 31, 2023:

Status of applications received with a Risk Assessment Form (RAF)	
7.7 %	Applications **rejected** due to research security administrative review
0.6%	Applications **still under evaluation**
57.9%	Applications **funded** by NSERC without requiring national security risk assessment
29.8%	Applications **not funded** due to program administrative or merit review
4%	Applications **referred to** national security agencies for risk assessment and advice

78% of rejected applications were successfully resubmitted

Funded applicants must implement their mitigation plan

Out of 48 applications
*2 were **withdrawn***
*14 were **funded***
*32 were **not funded***

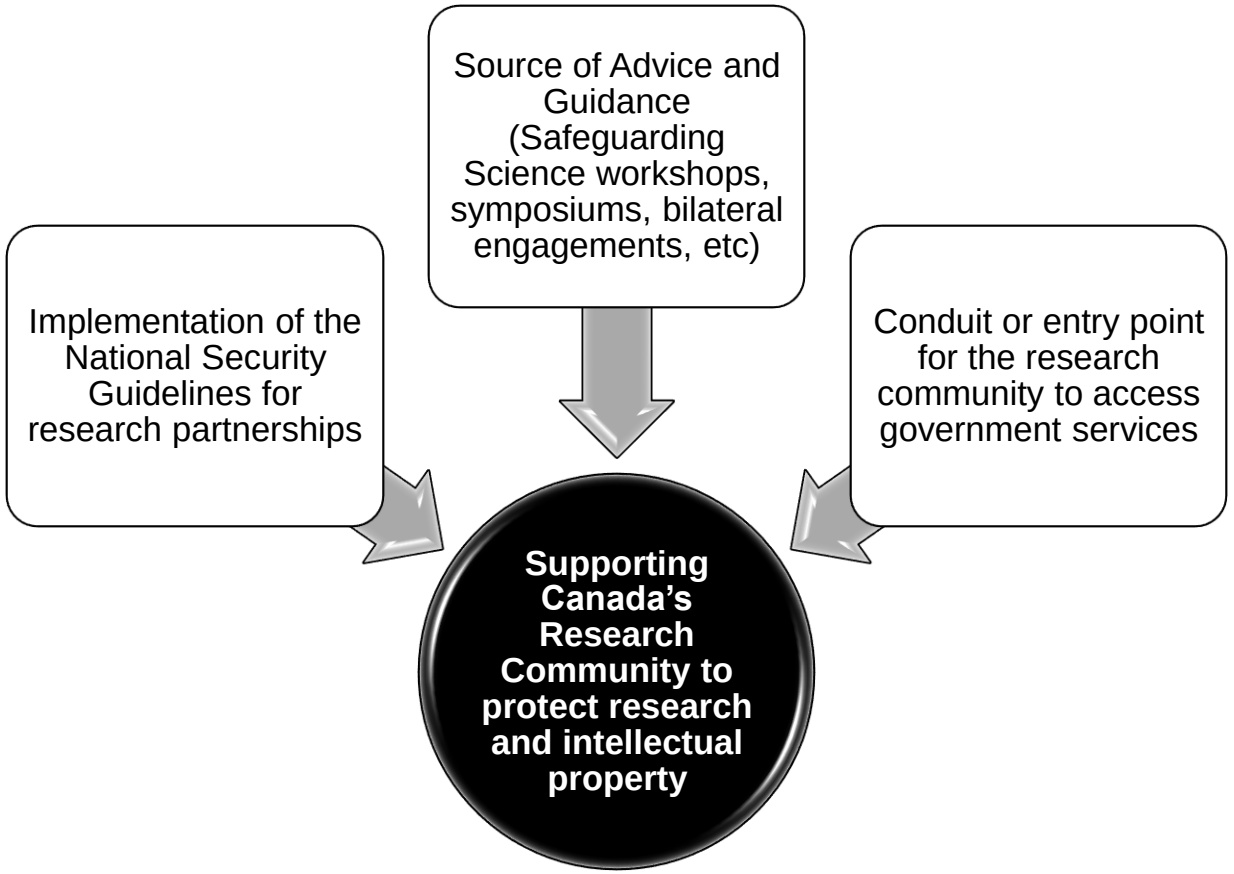
- NSERC's administrative risk validation **adds on average 1-2 days to the processing time of ~96% of Alliance applications.**
- **Processing time was exceptionally delayed in the ~4% of cases** where applications required advice from the national security departments and agencies; processes have improved, and clearer service standards will be set.
- **Success rates for applications to the Alliance program have not changed**. including for applicants who self-identified as a visible minority.

Impact of the NSGRP on NSERC's Alliance grants program

- The **pilot stage** of the NSGRP in NSERC's Alliance grants program is completed. Impact includes:
  - ~40% of grants funded with no risks identified
  - ~60% of grants funded with risks identified, appropriately mitigated by a **risk mitigation plan**
- Lessons learned and community feedback led to an updated Risk Assessment Form in March 2023. with increased clarity and usability, and with greater focus on EDI and **non-discrimination**.
- New resources developed based on the pilot such as the Open-Source Due Diligence Guide (published in 2023). More resources upcoming (e.g., improved risk mitigation guidance).
- First annual **Progress Report** on the Implementation of the NSGRP will be published this Summer.
- The next phases of implementation will be **gradual, risk-based,** and **limited** to funding opportunities that support partnerships. Further details will be announced in funding opportunity literature.
  - To date, the NSGRP were also introduced to the second stage of the joint Canada Biomedical Research Fund and Biosciences Research Infrastructure Fund competition.

Canada's *Research Security Centre*

Research Security Centre - Overview



Research Security Centre - Structure

Tools Development and Guidelines Implementation Team

Team of 5 based in Ottawa

1. Lead PS's role in implementing the Guidelines (high-risk assessments)
2. Develop, update, maintain and disseminate research security tools
3. Liaise with regional advisors to update tools using stakeholder feedback
4. Coordinate activities within the federal government, and with external stakeholders (P/Ts, academia, private sector, allies)

Advice and Engagement Team

Team of 6 Regional Advisors and 1 manager (at HQ)

1. Directly engage and establish networks with research institutions, industry partners, and P/Ts
2. Liaise regularly with S&I partners
3. Deliver Safeguarding Science Workshops
4. Assist researchers with Guidelines, other queries related to federal departments and agencies

The Centre is partially operational

Research Security Centre - Structure

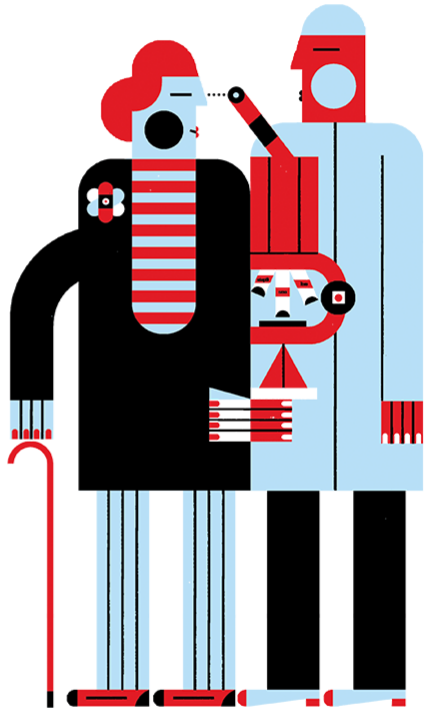
Currently staffed Regional Advisors (RAs)

- Edmonton (Erin Dorgan)
- Greater Toronto Area (Todd Bielarczyk)
- Waterloo (Jennifer Weese)
- Victoria (Nigel Fitch)
- Quebec City (Laurie-Eve Rioux)

To be staffed by summer 2023

- Halifax

New policy directions & next steps



New Research Security Policy

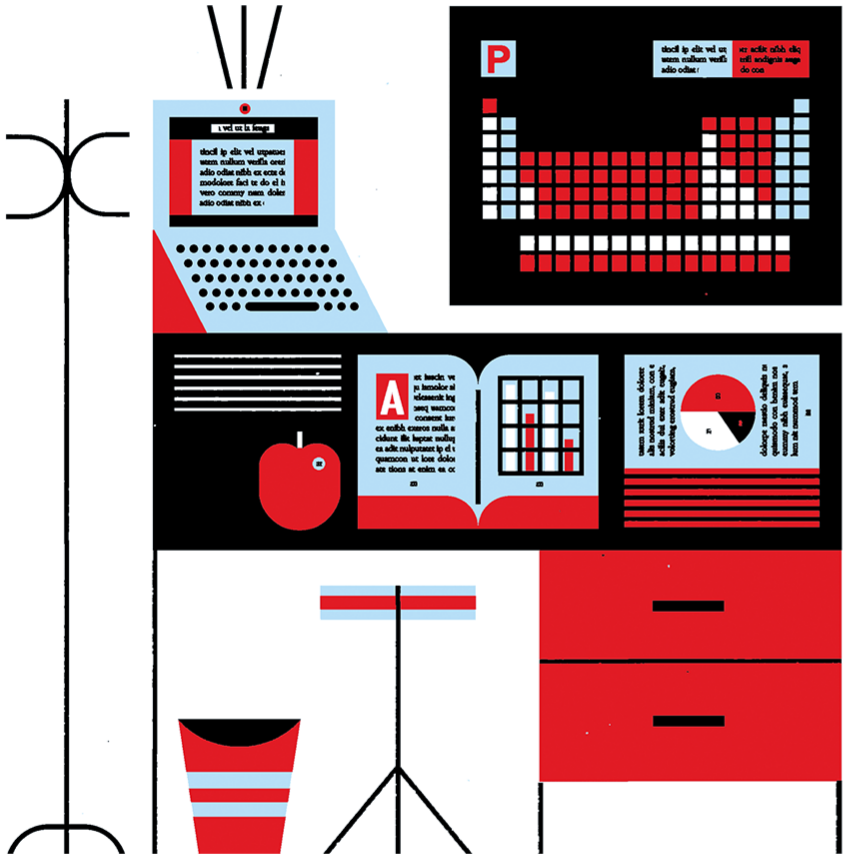
In February 2023, a new tri-ministerial statement on protecting Canada's research requested **new measures:**

*"Research grant applications proposing to conduct research in a **sensitive research area** will not be funded if any of the researchers working on the project are **affiliated** with a **university, research institute or laboratory connected to military, national defence or state security entities** of foreign state actors that pose a risk to Canada's national security."*

The federal granting agencies (NSERC, SSHRC, CIHR) and the CFI are working in close collaboration, alongside Government of Canada partners and the GoC-Universities Working Group, to develop the requested policy approach and assess its impact on our processes.

New Research Security Policy

- Starting in March 2023, NSERC has notified researchers and institutions about the upcoming measures by appending a letter on **enhancing Canada's research security** to all Notices of Decision (NODs) of research grant awards**.** The letter and a Frequently Asked Questions document have also been shared with research grant offices.
  - A similar approach is being followed by the other granting agencies.
- Significant work has been underway to develop a **risk-targeted**, **science-appropriate**, and **transparent** policy, with clear definitions, guidance, and lists for use by the research community.
- **This policy is distinct from the NSGRP and has not yet been implemented**.
- Clear guidance and timelines will be provided by the Government of Canada and by federal granting agencies to ensure that the research community can understand and comply with the new policy.



Questions?

Shawn McGuirk

Research Security

shawn.mcguirk@nserc-crsng.gc.ca

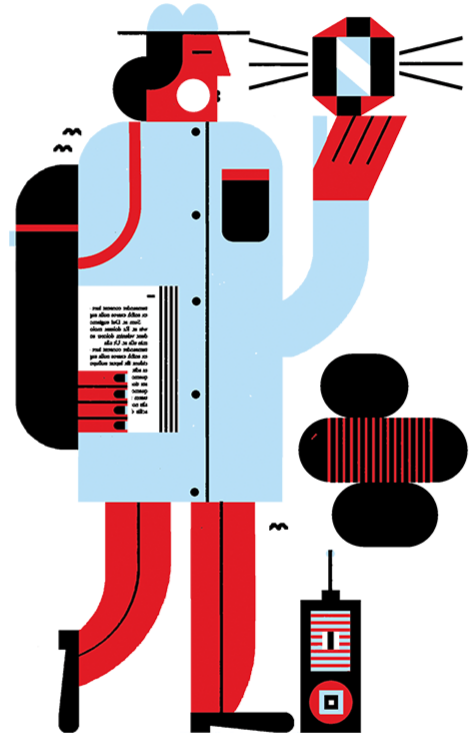
researchsecurity@nserc-crsng.gc.ca

Connect with us

@nserc_crsng

facebook.com/nserccanada

Bonus Material



March 24th 2023 Risk Assessment Form Updates

Update

- Innovation, Science and Economic Development (ISED) Canada, in consultation with the federal granting agencies and the national security departments and agencies, has updated the Risk Assessment Form (RAF).

- On March 24, 2023, the updated RAF was posted on the Safeguarding Your Research portal, replacing the previous version.

- Changes to the RAF were informed by feedback received from the research community, including by a survey on the implementation of the National Security Guidelines for Research Partnerships (Guidelines) conducted by the U15 Group of Canadian Research Universities and Universities Canada in Summer 2022.

Key changes

- **Questions —** All questions have been streamlined and rephrased for greater clarity. Additional information was added to help applicants complete each question and to reduce the need for them to refer to separate documents or pieces of legislation.
- **Risk Assessment Process —** The “Overview of the Process” and “Process flow chart” that were in appendix to the original RAF have been removed. This information was updated and is now presented on a new **Risk Assessment Review Process** page of the Safeguarding Your Research portal.
- **Annex A (Sensitive Research Areas) —** To more easily hyperlink to sections of Annex A within the Risk Assessment Form, the list of sensitive and dual-use research areas and sensitive personal data in the Annex have been integrated into two distinct tables.
- **Risk Mitigation Plan Information —** The information on risk mitigation was removed from the new RAF, and it is now presented on a new **Mitigating Your Research Security Risks** page on the Safeguarding Your Research portal.

Changes to “Know your research”

- Questions were re-ordered so that the indicator-specific questions (i.e., reference to existing lists) come first and the reference to the sensitive research list in Annex A of the Guidelines comes last.

- The question on sensitive personal data and large amounts of data was split into two new questions (i.e., questions 1.3 and 1.4).

- Question 1.5 was added to determine if the research area is related to goods or technology that are included on the *Export Control List* of the *Export and Import Permits Act* (EIPA).

    - All previous questions about import / export / controlled goods lists, and the section “Know your EIPA obligations”, have been removed.

Changes to “Know your partner”

- Two questions from the previous iteration of the form referenced risk factors that had no possible mitigation measures, and so have been removed.
- These risk factors were instead integrated into a new section 5, “**Additional Requirements**”, which now states:
  - “By submitting this Risk Assessment Form, the applicant on behalf of all co-applicants agrees that, to the best of their knowledge:
    - The applicant(s) have not accepted and will not accept any offer of funding that is conditional upon the mirroring of their academic laboratory in, or the transfer of their academic laboratory to, a foreign country; and
    - The source of funding and the value of the research project to the partner organization(s) has been communicated by the partner organization(s) to the applicant(s).”

Changes to “Know your partner”

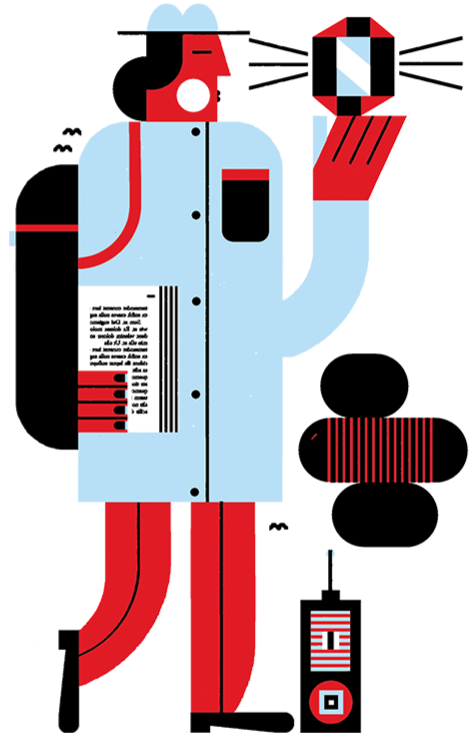
- The question “Your partner organization has been charged, admitted guilt, or has been convicted of fraud, bribery, espionage, corruption, or other criminal acts that could speak to a lack of transparency or ethical behaviour” was revised and included as an indicator to question 2.2.
  - The description further clarifies that applicants should search for events within the last five years

- The question “There is information to suggest that conflicts of interest or affiliations exist for any research team members that could lead to transfer of research to third party governments, militaries, or other organizations” was rephrased in question 2.3.
  - The scope of this question is **limited to partner organization personnel** involved in the project as well as their supervisors, managers, and executives
  - The **partner organization should be consulted** regarding any real, perceived or potential ties of said individuals to foreign governments/militaries in order to accurately respond to this question

Changes to “Know your partner”

- The question “Your partner organization will have access to Canadian facilities, networks, or assets for conducting the research unrelated to this specific partnership” was rephrased to question 2.4.
  - It asks if your partner organization will gain access to your institution’s infrastructure or data unrelated to this project ***because*** of this specific partnership.
  - **This question does not ask if your partner organization already has legitimate access to infrastructure or data at your institution due to other partnerships or projects.**

Best Practices



Open Source Intelligence (OSINT) Due Diligence

- A new **Guide on Conducting Open Source Due Diligence** is now available on the Safeguarding Your Research Portal.
- The goal is to verify that your research partners are who they say they are and to ensure their relationships and motivations are clear
- OSINT due diligence helps you find some risk indicators like:
  - Structures or relationships that may compromise your partner's autonomy
  - Indications of connections to foreign governments, militaries or security services on sensitive research areas
  - Information that shows your partner operates in countries known to steal intellectual property from researchers
  - Any information that suggests lack of transparency

Risk Mitigation Plan

Mitigation measures should be tailored to the research project and commensurate with the risks identified while considering open science principles. Mitigation plans can cover areas, such as, but not limited to:

- **Describing any other relevant review processes for which the project has been subject to.**
  e.g., Has your project been reviewed by any internal committees to determine how the data should be specifically safeguarded?
- **Raising research security awareness and building capacity across your research team**
  e.g., Have you committed to providing training to members of your research team around Research Security related topics?
- **Ensuring that your partner organization(s)' objectives align with the objectives of the partnership**
  e.g., Have you discussed with your partner what they hope to gain from the partnership?
- **Ensuring sound cybersecurity and data management practices**
  e.g., Are there device management protocols for professional and personal international travels occurring during this project?
- **Agreement on the intended use of research findings**
  e.g., How will Intellectual Property be handled with your research team, your collaborators, and your partner organization(s)?

Recommendation

“The evolving research security landscape requires ongoing dialogue between all parties in the research ecosystem, in Canada and globally, to grow our shared capacity to identify and mitigate risks while upholding the principles and values that enable open research and foster EDIA.”