Gouvernement du Canada | Government of Canada

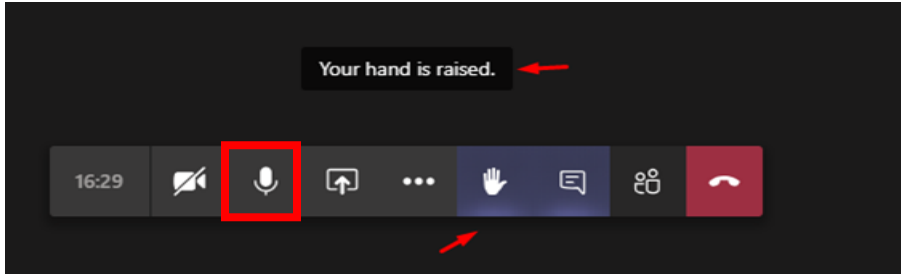
Canada

Safeguarding Science

Raising Awareness of Security Risks in Research Environments

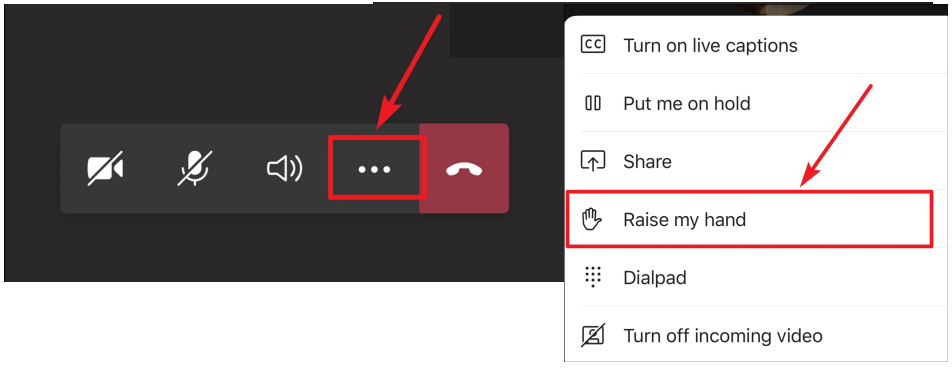
Instructions

1. Please **mute** your microphones.



2. Please use the **raise your hand** feature or the **chat** function to pose questions or comments.

3. For mobile users, please use the **three dot button** to raise your hand.



House Rule

- All discussions to be conducted under Chatham House Rule to facilitate an **open and frank** discussion.

- This is an interactive presentation where your input will be sought, so we **encourage participation.**

Workshop Outline

1. Safeguarding Science Presentation

- Key Concepts
- The Threat Picture (CSIS)
- Advancing Open Science and Security
- Vulnerabilities
- Resources and Ongoing Work
- Key Takeaways

2. Discussion (Q&A)

3. Risk Assessment Form Presentation

Objectives

1. Raise your **awareness** of the threats faced by Canada's research community, as you apply for CBRF/BRIF.

2. Bringing to your attention security concerns that could be implemented into the adjudication process of research funding decisions.

3. Offer resources that the Government of Canada has developed and is working on.

Key Concepts

PROLIFERATION

The spread of *weapons of mass destruction* (WMDs) to or by state and non-state actors; their delivery systems; or the goods, technologies, or information applicable to the development of such weapons and systems.

DUAL-USE

Research or commodities with the potential to be used for both benevolent (legitimate) and malicious purposes.

Key Concepts

INSIDER THREAT

The potential for anyone who has knowledge of or access to an organization's infrastructure and information and who could use that, either knowingly or inadvertently, for illegitimate purposes or to cause harm.

OUTSIDER THREAT

The potential for an individual or group who does not have authorized access to an organization's assets to act in a way that could lead to the illegitimate acquisition of assets or to causing harm.

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Research Security
Protecting Canadian Data Science & Technology

Canada is a global research leader, due to our world-class universities, public and private research organizations, and human talent.

Canada's innovative reputation attracts threat actors: they exploit our principles of open science and collaboration; disregard Canada's laws and values; and disguise their role in serving a foreign state agenda to obtain valuable Canadian data, intellectual property (IP) and know-how.

These deceptive and malign activities harm Canada's safety, security and prosperity interests. Canada's research integrity is undermined; our knowledge-based economy is stolen; and threat actors gain powerful and destabilizing surveillance and military capabilities.

UNCLASSIFIED

Who & Why

- Hostile state actors, particularly China and Russia, pose the greatest threat.
- In our digital era, threats can arise from anywhere, including from non-state actors.
- The world is increasingly competitive. Hostile states seek advantage at Canada's expense. They look to advance their economic, technological, intelligence and military state interests.
- Policies and practices of Military-Civil Fusion, coercive national security laws, and state capitalism pose a growing threat.

What

Almost all Canadian research domains face some level of risk; but the top five targets are:

- Biopharma & health
- Artificial intelligence (AI), quantum, and big data
- Semiconductors, 5G, and smart cities
- Ocean technology, including sensors
- Aerospace technology, including hypersonics

How

Sophisticated threat actors will exploit vulnerabilities, including via deceptive means, such as:

- Traditional espionage
- Cyber espionage
- Insider threats
- Non-traditional collectors
- Talent spotting
- Research funding
- Unsafe supply chains *(equipment, services)*
- Joint ventures
- Minority investments *(e.g. venture capital)*
- Foreign acquisitions *(foreign direct investment)*

SENSITIVE LABORATORIES — Threat actors seek direct or indirect access to sensitive laboratories.

INTELLECTUAL PROPERTY (IP) — Control over IP may be lost, with all gains accruing to foreign states.

DEFENCE & DUAL-USE — Researchers may knowingly or unwittingly contribute to foreign military capabilities

ACADEMIC LEADERSHIP — Leading academics and administrators may be targeted or leveraged.

RESEARCH GRANTS/ FUNDING — Government funding may be subverted, and foreign funding may co-opt Canadian research and IP.

These threats are real; and Canada is not unique in managing these challenges and risks.
Most importantly, you are not alone in facing these threats.

613-993-9620 (24/7) • https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

Canada

Advancing open science and security

ENCOURAGE A COOPERATIVE AND OPEN RESEARCH ENVIRONMENT

Security Considerations

"AS OPEN AS POSSIBLE AND AS SAFEGUARDED AS NECESSARY"

Vulnerabilities: Dual-Use Technologies

BIOLOGICAL AND CHEMICAL

Development of biological agents:

- Modified mousepox virus
- Creation of transmissible agents (e.g. h1n1)

Development of chemical agents:

- Pesticides
- Pharmaceuticals (e.g. fentanyl)

RADIOLOGICAL AND NUCLEAR

- Triggered spark gaps
- Novel alloys/ composites
- Mass spectrometers
- Variable frequency drives
- Induction furnaces

MILITARY

- Accelerometers
- High-power lasers
- Inertial navigation systems
- Satellites & spacecrafts
- Thermal imaging systems
- Fluid dynamics
- Electromagnetic spectrum absorbing materials

Vulnerabilities (continued)
What type of information are we concerned about?

Information that…

- ✓ Is novel;
- ✓ Has significant intellectual property considerations;
- ✓ Has the potential to be used in military or weapons programs;
- ✓ Is personal information that puts Canadians at risk;
- ✓ Has strategic economic or national security value

RESEARCH DATA THEFT

- Proprietary data and information
- Insights and supplementary data

INTELLECTUAL PROPERTY THEFT

- Detailed schematics/manuals/formulas
- "Trade secrets" and performance data
- Physical products or samples
- Knowledge and research materials

PERSONAL INFORMATION THEFT

- Daily life or schedule patterns
- Login information or other credentials
- Compromising/embarrassing information
- Personal information collected in research relating social sciences

Government of Canada Resources

Regional Resilience Assessment Program (RRAP)

- The RRAP is an all-hazards risk assessment program that provides non-regulatory guidance and solutions to critical infrastructure owners and operators.

ISED's Safeguarding Your Research Portal

- A portal that aims to provide the research community with guidance, information and tools to help them protect their research and intellectual property.
- Recent addition of two online courses and the GoC's National Security Guidelines for Research Partnerships.

The Canadian Cyber Security Tool (CCST)

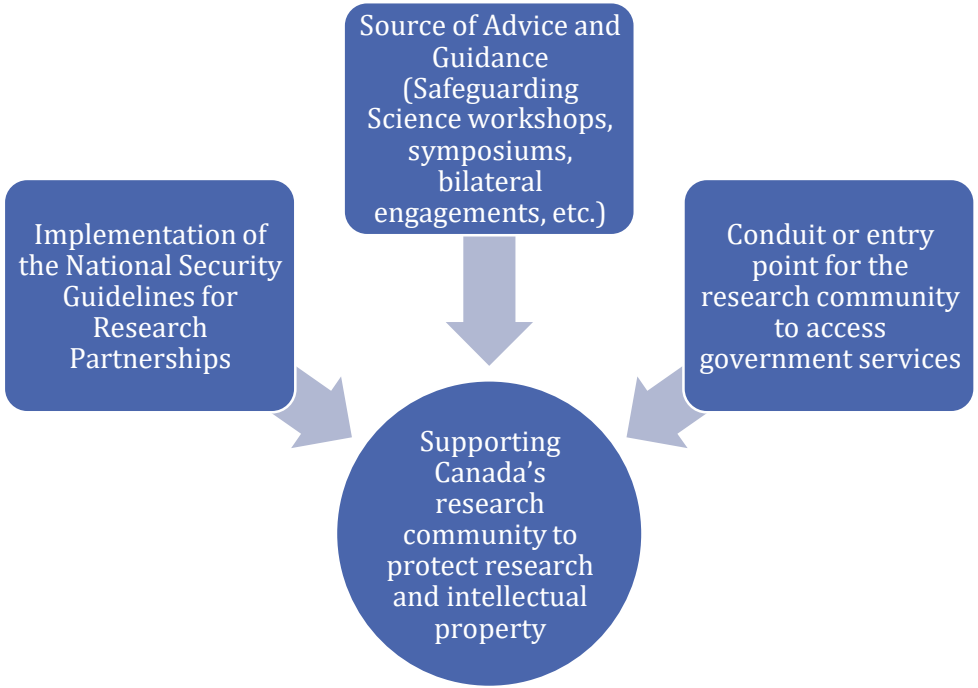
- A virtual self-assessment tool that provides the participant with an overview of their organization's operational resilience and cyber security posture, as well as comparative results across their sector.

Government of Canada Resources
(continued)

Research Security Centre

Consists of 2 teams:

- **HQ Team**
  - Tools development
  - Implementation of the *National Security Guidelines for Research Partnerships* and new RS policy
- **Regional Advisors Team**
  - Outreach and advice to universities, P/Ts and academic institutions
  - Situated in Toronto, Victoria, Waterloo, Edmonton, Quebec City, Halifax



Ongoing Work and Recent Developments

- Implement the *National Security Guidelines for Research Partnerships*.

- Implement February 14 – Ministerial statement *"Grant applications that involve conducting research in a **sensitive research area** will not be funded if any of the researchers working on the project are **affiliated** with a university, research institute or laboratory connected to military, national defence or state security **entities** of foreign state actors that pose a risk to our national security.*

- Aiming for the Centre to be fully staffed and operational by summer 2023.

- Regional Advisors to continue to establish themselves and consult with universities and provinces on the services the Centre can provide.

Key Takeaways

Security threats and proliferation concerns are real.

Research, data and products are highly valuable and equally vulnerable.

Important to be mindful of the risks and security considerations when applying for research grants.

It all comes down to awareness and asking questions to learn more.

Thank you for attending the workshop!

If you have any additional questions or feedback, please email researchsecurity-securiteenrecherche@ps-sp.gc.ca.