CONFERENCE REPORT

2025 RESEARCH SECURITY CONFERENCE

Navigating New Domestic and Global Frontiers

Vancouver, June 3-4

THE UNIVERSITY OF BRITISH COLUMBIA

CONTENTS

Acknowledgement

The 2025 Research Security Conference was held from June 3-4, 2025 at UBC's Point Grey Campus, which is located on the traditional, ancestral and unceded territory of the xwməθkwəy̓əm (Musqueam). Conference attendees and speakers also joined from lands near and far; we also acknowledge the traditional owners and caretakers of those lands.

PREFACE

This report was produced to summarize the major discussions of the 2025 Research Security Conference. To protect the confidentiality of the conference participants, the organizers enacted the Chatham House Rule, whereby the statements of the speakers can be shared and discussed, however the identity of the speaker should remain anonymous. Furthermore, the conference organizers refrained from using electronic recording or artificial-intelligence assisted note-taking, in respect of protecting the privacy of the speakers and security of the information shared. The summaries enclosed below were produced from handwritten notes taken by the event organizers, and were therefore subject to the interpretation of the listener. The information presented should not be taken as fact without further consultation with appropriate experts and professionals in research security and related fields.

EXECUTIVE SUMMARY

The University of British Columbia (UBC) hosted the *2025 Research Security Conference: Navigating New Domestic and Global Frontiers* from June 3-4 at UBC's Point Grey Campus. This conference intended to build capacity and share information among a growing Canadian community of research support professionals focused on research security.

The conference included in-person participants from:

- 54 Canadian post-secondary institutions, of which 34 were from non-U15 universities, colleges and polytechnics;
- 12 Government of Canada departments and agencies;
- four provincial governments;
- 13 civil society organizations and major national research facilities;
- six international entities from Australia, Germany, Japan, the United Kingdom and the United States of America; and
- three private sector companies that provide research security-related services.

Across two days of discussions, panels and breakout sessions, the conference showcased a variety of approaches and considerations when designing and implementing research security programs and policies at various institutions. Conference participants benefited from a wealth of knowledge that spanned multiple sectors, while engaging in idea-sharing and open dialogue on how to address important shared research security questions.

Breakout sessions allowed participants to choose among research security themes most aligned with their professional interests. The panels and discussions covered a wide variety of topics, such as best practices for conducting open-source due diligence, supply chain risks, capacity building and international approaches to safeguarding research. The sessions also featured speakers from a range of institutions and regions.

Multiple sessions addressed the downstream effects of research security challenges that can arise within the research and academic landscapes. These effects include impacts on institutional policy, researchers' perceptions of collaboration and the ability to recruit and retain international students, in particular since the introduction of the Government of Canada's Policy on Sensitive Technology Research and Affiliations of Concern (STRAC) and the expansion of the National Security Guidelines for Research Partnerships (NSGRP) in May 2024.

TAKEAWAYS AND RECOMMENDATIONS

1. Openness in research is critical to maintaining Canada's research competitiveness. Canada must engage with international partners to be successful and participants reiterated that open research and research security go hand-in-hand.

2. Canada's policy-related resources and guidelines, such as the named research organization (NRO) and sensitive technology research areas (STRA) lists, are informing the global development of research security frameworks. However, with greater global adoption of research security practices and their related administrative requirements, researchers and institutions can struggle to navigate various overlapping but sometimes disparate frameworks. It would therefore be advisable for jurisdictions to align requirements whenever possible.

3. Funding for research security programs in Canada through the Research Support Fund (RSF) has been critical in building capacity at many institutions. However, smaller institutions have limited (financial) resources and struggle to fully address emerging issues or build research security capacity. Furthermore, while research security considerations and their related administrative requirements have increased steadily in recent years, the total funding dedicated to research security in the RSF (CAD 25 million) has not changed. Given increasing research security and attendant administrative requirements, small and medium sized institutions, in particular, could benefit from additional resources and support form relevant governments.

4. The implementation of the policy on STRAC and the NSGRP have provided Canadian universities and research organizations with a useful framework for implementing practices to safeguard research and mitigate risk while conducting their world-leading research. Research security professionals from across Canada continue to engage in information-sharing and competency-building measures (e.g., webinars, workshops for analysts) to help clarify government policies and guidelines.

5. The Canadian research community, including institutional administrators and researchers from across the country, has observed unintended effects from the implementation of the policy on STRAC and the NSGRP. Some of these effects appear to be tied to misunderstandings related to the frameworks; for example, as some conference attendees shared:

    I. Some researchers have assumed that all research partnerships with NROs will be ineligible for federal government funding, regardless of the sensitivity of the research. Furthermore, some researchers may avoid certain partnerships in select jurisdictions (e.g., the People's Republic of China) altogether, assuming that all such engagements are prohibited. This is in spite of the fact that the policy on STRAC does not prohibit such engagements;

    II. Researchers, in particular principal investigators, may assume that they will experience increased scrutiny from funding agencies or government entities for hiring graduates from a NRO, regardless of whether their research is advancing a sensitive technology research area or receiving Canadian federal funding. Some of these concerns are likely driven by certain province-specific guidelines. Early-career researchers and international students may be uniquely affected by these assumptions.

6. The informal community of practice, convened as "Team Canada" as a network of research support professionals, provides a model for how to strengthen research security approaches at post-secondary and other institutions through collaboration. Region-specific and smaller communities of practice can also offer considerable value.

KEYNOTE SUMMARY

The keynote focused on engagement with research institutions in the People's Republic of China (PRC), many of which have rising research profiles or are already globally recognized as leaders in certain fields. According to data from the Organization for Economic Co-operation and Development (OECD), the rise of the PRC's research sector coincides with a 164 per cent increase in research and development spending between 2012 and 2023. In comparison, increases in research and development spending in countries such as the United States (68 per cent increase), Canada (26 per cent increase), and Japan (17 per cent increase) have not matched the PRC's, thereby limiting the sector's growth.

Several institutions in the PRC have also been subject to research security related concerns, given the country's adoption of policies that promote civil-military fusion and close collaborations between some institutions and the People's Liberation Army. The keynote also noted that while there are many factors and actors to consider when evaluating risks related to research security on a global scale, entities based in the PRC posed the most significant concern.

Many institutions within the PRC have increased their publication intensity and have experienced a subsequent rise in international rankings for innovation and scientific development. Much of this activity has focused on emergent technologies deemed sensitive by governments such as the United States and Canada. These trends reflect top-down direction from the PRC government and conscious efforts to increase central state management and priorities in scientific development, so as to push Chinese institutions to the forefront and to domesticate important areas of research and development.

The term "sensitive research" now encompasses a wide range of research areas. Some technologies that are being targeted by malign actors for theft or misappropriation do not neatly fit within traditional definitions of "dual use" technologies. Some targeted technologies, for example, are sensitive because they are critical to economic development and competitiveness. As such, there is a need to develop a new paradigm to safeguard these types of technologies given their importance.

The speaker stressed that governments and institutions must consider a variety of tools to improve research security. One model that many jurisdictions have adopted is a "compliance plus" model, whereby a mix of regulations, requirements and incentives is used to compel those involved in research to take measures to prevent unauthorized transfer of sensitive research and knowledge.

To be effective, this model requires continuous collaboration and engagement across domestic and international sectors. This may mean sharing risk analyses and best practices while continuing to engage and educate researchers to navigate the uncertainties.

PANEL SUMMARIES

The conference featured seven panels over two days, as well as a brief introductory presentation to set up the breakout sessions. The below information summarizes discussions related to the panels but is not a comprehensive record of all comments presented at the event.

Panel #1: View from the Agencies One Year Post-STRAC

MAIN TAKEAWAYS

- Researchers are increasingly aware of administrative requirements related to the policy on Sensitive Technology Research and Affiliations of Concern (STRAC) and National Security Guidelines for Research Partnerships (NSGRP).
- Researchers and research administrators exhibit less risk-avoidance, and increased awareness of risks and corresponding mitigation measures in the one year since the policy on STRAC's implementation and the expansion of the NSGRP.
- Federal funding agencies noted a significant decrease in rejected proposals due to unmitigable research security-related risks and an increase in outreach and engagement from universities on research security topics.

SUMMARY

This panel included representatives from most of Canada's federal research funding agencies and government departments working directly on research security frameworks. Panellists announced that expected updates to the NRO and STRA lists are planned for Fall 2025 and that the NSGRP will now apply to select funding opportunities offered by the Social Sciences and Humanities Research Council (SSHRC). Of note, government panellists indicated that social science-related research areas may be included in future updates to the list of sensitive technology research areas.

The panel reported significant improvement in the quality of risk mitigation plans since the NSGRP was launched as a pilot program in 2021. They observed a decrease in the submission of the highest risk proposals, with only four proposals having been rejected due to national security concerns over the past year (at the time of the conference, a public report on the program outcomes was forthcoming).

Over the second half of 2025, the NSGRP is anticipated to apply to an increasing number of partner-based grants, and SSHRC shared their definition of "private sector partner" that will guide their implementation of the NSGRP. The funding agencies will also begin to validate STRAC attestation forms per their published guidance.

Panellists also noted that infrastructure-related research funding covering longer timespans, such as that from the Canada Foundation for Innovation, requires a unique approach to research security. For example, project teams may encounter challenges in identifying potential affiliations to named research organizations in cases where some participants in the project do not have "named roles" as part of the grant application. Project teams

may need to raise awareness of research security more broadly amongst the team and adopt a more holistic posture to support effective risk mitigation, as a result.

Engagement with the academic community and stakeholders from Public Safety Canada and national security departments plays a vital role in the research security ecosystem. Research security-related security threats have evolved and do not primarily target government institutions and representatives; security risks now include direct threats to and from non-state actors, which can include researchers and research institutions. The implementation of the provisions passed in the Government of Canada's Bill C-70, *An Act respecting countering foreign interference*, will allow national security agencies to share important risk-related information with researchers and academic institutions. The Government of Canada is currently formalizing an information-sharing framework based on the bill.

Panel #2: View from Researchers in Sensitive Technology Research Areas

MAIN TAKEAWAYS

- Researchers are struggling with some of the ramifications of research security policies and guidelines, particularly regarding student mobility, international recruitment, and international collaborations.
- There is a desire for increased transparency in the immigration visa and security clearance process as it relates to research security.
- Research security policies can disproportionally impact early career research faculty; these faculty rely on predictable and straightforward student recruitment to support their work.
- Researchers often err on the side of caution when making decisions about collaborations, which can lead to forgoing collaboration and talent opportunities that would not otherwise be prohibited under the policy on STRAC.

SUMMARY

Three researchers from multiple institutions expressed their concerns about delays in security clearances for students working on some federally funded grants that require such clearances. Based on their experiences, they explained that these delays prevent researchers from beginning their work in full until their entire research team is cleared and there appears to be a lack of transparency about processing delays. Researchers also face similar uncertainty about delays in the visa approval process that can deter them from recruiting students or collaborators from certain regions and research organizations.

Participants expressed that an intended but unfortunate outcome of the publication of Canada's NRO list is that many researchers have needed to end collaborations and restructure decades-long networks. Effects on networks extend beyond active affiliations because researchers are worried about being perceived as contravening the policy on STRAC even when they adhere to co-publication guidelines. Researchers mentioned that accepting visiting scholars can be particularly challenging to navigate when visitors may retain active affiliations to NROs.

The panel discussed the perception of a "chilling effect" on hiring diverse team members due to fears of being found in contravention of the policy on STRAC. Worried about potential implications on their funding, many researchers would rather cease or avoid hiring graduates from an NRO altogether, even when doing so would encourage greater equity, diversity and inclusion on their team. In the context of a global competition for talent in science, technology, engineering and math disciplines, researchers regularly receive many applications for enrollment from talented students from countries such as the PRC and Iran—countries with institutions on the NRO list where prospective students may have affiliations. This competition, particularly among engineering and computer science disciplines, creates a limited window of opportunity to extend enrollment offers. The additional time it takes to ensure compliance with research security policies, combined with long delays in post-pandemic immigration processing, drastically narrows this window of opportunity. To prevent highly talented researchers from bypassing opportunities in Canada, the processes for institutions and government departments to confirm compliance with relevant policies need to become more efficient.

Panellists also emphasized the need to further strengthen the understanding of, and culture around, research security across all levels of post-secondary institutions, including within Faculties and departments. Strengthening the culture of research security will also help the next generation of researchers) to understand the potential implications of their educational and network decisions and make prudent choices that support the aims of research security earlier in their careers.

Panel #3: Navigating Provincial Research Security Requirements

MAIN TAKEAWAYS

- Each province has unique considerations when developing and implementing research security policies, including: the number of higher education institutions, types of tertiary education, population levels, and levels of funding support.
- Research organizations should not expect complete harmonization of provincial research security requirements between provinces or with the federal government, though provinces do engage in discussions with their federal counterparts.
- Provinces that are currently considering implementing research security frameworks are trying to reduce the burden on inter-provincial collaboration where possible.

SUMMARY

Ontario:

The Government of Ontario set a precedent in research security policy in Canada with its 2019 analysis of the Ontario Research Fund portfolio. The panel discussed the evolution of provincial efforts, whereby applicants initially did not receive feedback as to why their proposals were rejected, including which risks could and could not be mitigated, to more recently providing a fulsome disclosure of risks.

The Ontario government requires complete disclosure of Principal Investigator and/or co-investigator

involvement with foreign entities when assessing research security and is the first provincial government to make academic research security policies a legislative requirement under its *Supporting Children and Students Act*, 2025. As a result of this legislation, institutions risk losing funding in the event of non-compliance. Furthermore, partner institutions in other provinces are also impacted by Ontario government requirements when collaborating in specific scenarios.

The province currently does not provide additional funding to help institutions implement the new requirements, and various participants noted this is unlikely to change. In the question period following the panel, participants shared that while they do not disagree with Ontario having its own research security framework beyond the national framework, a lack of direct financial support from the province for research security can place increased pressure on institutions and negatively impact their ability to address requirements, both in Ontario and outside the province, when addressing the Province of Ontario's research security concerns.

Quebec:

Quebec has many small institutions that face severe resource constraints; this challenges their ability to implement research security programs. Research security-related discussions began in 2023 between the provincial ministry that funds post-secondary institutions and the ministry that funds research. The Government of Quebec aims to model their provincial policies on the federal guidelines while recognizing unique provincial considerations.

Manitoba:

The University of Manitoba plays a unique role in its provincial research ecosystem, as most of the province's population resides in Winnipeg, where the university is located. The University of Manitoba has approached research security intending to build a culture of research security awareness, education and support.

Alberta:

Universities in Alberta established a community of practice comprising 19 members—led by the universities of Calgary and Alberta—to assist institutions of all sizes in navigating the provincial and federal research security policies. The four largest research universities in Alberta continue to engage their provincial government to better understand its "China Pause" approach to all research activities, whereby all new research partnerships with entities linked to the Chinese government were placed on hold in the spring of 2021, and existing relationships were examined. The Government of Alberta adjusted its approach to the China Pause policy in 2023 to allow some low-risk engagements.

Panel #4: International Approaches to Safeguarding Research

MAIN TAKEAWAYS

- Research security, while a relatively new consideration for many countries that lacks a common definition, is gaining significant attention at the policy level by governments around the world.
- Globally, governments are beginning to establish frameworks, policies and procedures that focus on enhancing research security capabilities while still conducting collaborative and groundbreaking research.
- Many countries are inspired by Canada's policy on STRAC and its associated lists when developing their approaches.

SUMMARY

United States of America:

The National Science Foundation (NSF) began rolling out the use of harmonized disclosure forms in February 2024 and published a risk-review framework later that year to assist universities in conducting research security due diligence. Institutions that receive more than USD 50 million in federal research funding must certify to the funding agency that the institution has established and operates a research security program. Raising awareness is important to the NSF's approach towards research security; risks in research will never be zero.

The NSF aims to strike a balance between funding open science while mitigating security-related risks to the highest extent possible. To this end, they've supported the creation of the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) program (through a USD 67 million investment over five years). The SECURE program has two components: a SECURE Center led by the University of Washington and a SECURE Analytics team spearheaded by Texas A&M University. The centre will help create a "Shared Virtual Environment" so that researchers, officials and leaders can jointly identify and address research security challenges. The analytics team, on the other hand, will develop tools and technologies for information gathering, data compilation, storage and analysis related to the research security landscape and various types of security incidents. The analytics group will also provide training and support, and help develop risk assessment frameworks and reports on research security risks.

Japan:

In Japan, conversations around how to best safeguard research began in 2024 with a focus on research integrity. In 2025, with increased attention to research security, the government published more detailed research security guidelines based on the country's export control frameworks and established the Inter-University Cooperation Scheme (URSIC).

As of June 2025, URSIC counts eleven of Japan's more than 800 universities as members and is actively encouraging more institutions to formally apply. URSIC operates similarly to Canada's informal community of practice, known as "Team Canada," but is organized more centrally and comprises dedicated roles for its

members, such as supporting members in conducting due diligence. URSIC further helps with raising awareness on research security, developing human resources, supporting smaller institutions, and communicating with the Government of Japan and international partners.

Japan's Ministry of Education (MEXT) and the Japan Science and Technology Agency (JST) began piloting research security requirements and oversight on specific grants and launched research security-specific training resources in 2025, including the development and sharing of informative case studies to university administrative staff and researchers.

Germany:

The German federal government has not yet released a national strategy or framework for research security, but has been engaged in research security discussions for roughly five years. Academic freedom is protected as a fundamental right by Article 5 of Germany's constitution, which therefore frames many conversations around research security. The German government published a position paper on research security in March 2024, and in May 2025, the German Science and Humanities Council also published a report titled *"Science and security in times of global political upheaval."* Multiple funding agencies and government institutions have started (or are in the process of) implementing guidelines and advice on international research partnerships. There is also an active debate in Germany about the role of German institutions in domestic military research; this debate is connected to research security given the nature of defence research.

In early 2024, the Helmholtz Association, which represents 18 research institutions across Germany, realigned its policies related to research security. Helmholtz takes a country-agnostic approach to research funding and focuses on de-risking over de-coupling collaborations with international partners. To this end, Helmholtz centres are responsible for implementing "individual adequate security measures" at a local level. The centres are encouraged to look holistically at the risks related to research and partnership as opposed to widely prohibiting all institutions from certain collaborations. Various centres have taken their own approaches; for example, Forschungszentrum Jülich (FZJ) has implemented an administrative support service called "Due Diligence in Science" to help the institution assess opportunities and risks associated with proposed collaborations.

Australia:

The Australian Commonwealth Scientific and Industrial Research Organisation (CSIRO) funds research in space, AI, supercomputing and other areas to solve global challenges through innovation, science and technology. They have 51 research sites, 87 country partners, and receive 40 per cent of their funding from the Australian federal and territorial governments.

CSIRO approaches research security using three principles: 1) informed due diligence and governance; 2) education and collaboration; and 3) continuous review and audit. CSIRO aims to give researchers information and tools to make security-informed decisions, for example, through the "Research Engagement Sensitivities Tool 2.0." The organization has also gamified training by creating a "Security Quest" game to raise awareness

and educate researchers on potential research risks. CSIRO conducts regular reviews of these initiatives (among others) for their efficacy and refines them.

CSIRO recently established a mandatory training program on countering foreign interference and takes a similarly structured approach to broader research security training. This includes due diligence assessments, education on research security topics, and consistent project reviews and audits on CSIRO programs. The goal for CSIRO is to build an ecosystem to respond to potential security threats.

Panel #5: Key Case Studies and Lessons Learned

MAIN TAKEAWAYS

- In specific circumstances, research security issues can extend beyond administrative compliance with federal policies. For example, universities can face risks from non-funding related sources, such as certain visiting delegations, private-sector engagements, and individuals who may be acting on behalf of foreign governments.
- Due diligence undertaken by research security teams can help mitigate risks significantly within these contexts through the open-source identification of potential issues and the adoption of requisite measures to address challenges.
- In some cases, institutional policies and processes were changed due to efforts to enhance risk mitigation measures relating to research security.

SUMMARY

One case study involved an engineer from a university in the United States who was found guilty of 36 counts of false grant disclosures after an investigation revealed that the engineer was part of the PRC's Thousand Talents Plan[1]. The university in question worked with the United States Federal Bureau of Investigation (FBI) to understand how this fact was not identified by the university or disclosed before the investigation. This case resulted in updated university employment policies and new mechanisms for researcher dismissals, to prevent future policy breaches and reputational impacts. Additionally, the university increased due diligence related to the recruitment of candidates from what they define as "countries of concern."

Another case study involved a substantial visiting delegation that requested to visit a sensitive research lab in Canada outside of the usual business hours. The lab's project was very decentralized and included work with advanced biomaterials. The visitors were high-profile representatives from a mix of private-sector companies, with certain academic affiliations loosely linked to NROs and close relationships to a foreign government.

The Canadian university's research security group provided their risk assessment to their researchers, who decided to proceed with allowing the delegation to visit. The research security team implemented strict

[1] The Thousand Talents Plan (TTP) is one of a host of Chinese talent plan programs. Under TTP, the government of the PRC seeks to recruit foreign nationals to research at Chinese institutions. The government can then extract and exploit research findings to further national interests. For further information, see the FBI's description of Chinese Talent Plans, the US Senate committee report 'Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans', or the Public Safety Canada statement on TTP.

mitigation measures to reduce the risk, such as only allowing small groups of the delegation at a time to attend fully supervised tours, and electronic device management while in the laboratory space. The university has since updated its operational policies for visiting delegations.

Another Canadian university shared a case study about a private company registered in the Province of British Columbia that wanted to visit labs and facilities conducting advanced materials research. The company had contacted the university's partnership team to arrange a visit and also had operations in the PRC related to semiconductor and sensor components. Due to the obfuscated nature of the company, their intentions to partner in a sensitive research area, and other discrepancies that include personnel connections with a separate military supply company, the partnerships team did not further pursue the engagement.

A final Canadian case study involved a faculty member receiving a request from a scholar who expressed an interest in visiting a Canadian institution to audit courses so they could improve their teaching abilities, but whose ultimate request was for an invitation to a research lab. A due diligence analysis identified risks relating to both the research and the research partner, including research publications, patents and Patent Cooperation Treaty filings with clear dual-use civilian and military applications. When presented with these materials, the faculty member determined that the potential risks outweighed the rewards and decided not to offer a formal invitation to the scholar. The university has since changed its process to include a safeguarding-research review before signing a letter of invitation for visiting scholars.

Panel #6 Taking the Human Approach: Ensuring Access, Diversity and Non-Discrimination

MAIN TAKEAWAYS

- It is critical to be sensitive to the potential for discriminatory practices that may result from the implementation of research security policies.
- A major concern among participants was the potential for discrimination due to the perception that certain policies apply to entire countries or their citizens and that such discrimination must be avoided.
- Panellists proposed strategies to lessen the potential for discrimination resulting from adherence to the policies, including face-to-face conversations, taking the time to explain nuanced policy applications and investing in long-term relationship building with the research community.

SUMMARY

The policy on STRAC has had unintended consequences in relation to researchers' network-building and collaborations. There is a trade-off, especially for early-career researchers, between building their academic career through global networks with leading institutions/researchers and the potential for limiting their own career opportunities due to overly risk-averse attitudes. For many researchers considering the policies, the path of least resistance is often the default response. Researchers may even forgo collaborations with specific countries or in certain research areas to simplify adherence to research security policies. This is especially the case if researchers and institutions speculate which organizations may be added to future iterations of Canada's NRO list.

One panellist shared their best practices in this regard, which is to incorporate a non-discriminatory and legal human rights-based approach when providing research security advice to researchers. Further best practices include meeting with researchers face-to-face to establish better relations, spending extended time when policies are first introduced to confirm general understanding of policies and their rationales (even if that may mean longer or repeated meetings), assessing their own biases as a research security practitioner, and talking about decisions in terms of the balance of trade-offs and benefits. It is important to recognize the severe consequences that can be brought about by hasty decisions made to fast-track funding approvals: avoiding hiring or collaborating with all talent from a certain region can encourage discrimination and forego the opportunity to work with top-quality talent.

Panel #7: The Ripple Effect of Research Security Policies Across Contexts

MAIN TAKEAWAYS

- There is no one-size-fits-all solution for universities or research institutes looking to establish a research security program.
- One consideration is to first identify the existing cultures and policies of their institution and work within them to develop effective research security approaches.
- Existing institutional policies that can be effective risk mitigation measures include conflicts of interest, conflicts of commitment, and internal grant reviews and approvals.

SUMMARY

Discussions focused on implementing research security teams at large institutions, including advantages and challenges to establishing this new practice in long-established organizations where researchers are not accustomed to incorporating national security-related considerations into their work and processes.

A particular challenge echoed across the panel is universities' highly decentralized structure. This structure can pose difficulties in raising awareness of research security policies and practices. General awareness-raising, soft introductions and building personal relationships have garnered the most positive results for research security teams when collaborating and connecting with the many departments and faculties at their respective institutions.

Academic environments also provide a unique opportunity to contribute to more impactful research security approaches by leveraging evidence-based decision making and responding to pressing current events and geopolitical issues of concern. Staffing research security teams with a diverse range of backgrounds and skillsets (e.g., research backgrounds, government backgrounds, change management professionals, etc.) may provide institutions with a more well-rounded approach on how to effectively encourage the safeguarding of research while balancing academic freedom and open collaboration.

BREAKOUT SESSION SUMMARIES

Day 1, Session #1: Small to Mid-Size Universities

MAIN TAKEAWAYS

- Smaller institutions often do not have the resources to create teams or offices solely dedicated to research security. This context, combined with limited (or in some cases, no) dedicated federal funding for research security, creates unique challenges in establishing robust research security programs.
- "Small to medium-sized universities" is a broad category, and it is important to recognize that a one-size-fits-all approach cannot be applied to every institution under the umbrella.

Institutions should leverage any resources available for guidance and support, including advisors from Public Safety Canada (PSC) and communities of practice at the provincial or national levels.

SUMMARY

Many small- and medium-sized universities in Canada do not have an executive responsible for research and innovation, and some research security professionals in these institutions report directly to provosts. The professionals assigned to research security responsibilities at smaller institutions are often managing diverse portfolios; this negatively impacts their ability to provide uniform and dedicated research security support. Less dedicated support for research security through the Research Support Fund (RSF) compounds these challenges.

There is no clear definition of a "small to medium-sized" institution in a research security context, and many organizations that could be considered to fit into this category have robust and growing research portfolios. The diversity of these institutions, therefore, necessitates unique approaches to research security that are tailored to a specific institution's needs. Further research is required to better understand where challenges and opportunities exist within these environments.

Smaller institutions may also experience some advantages, such as a greater ability to influence culture change amongst researchers and leadership. In particular, the process of explaining the reasoning behind research security policies has been successful at encouraging compliance with federal policies, as opposed to a focus on the request to complete the required forms.

General advice for small and medium-sized institutions in accessing research security resources includes:

- Connect with the regional research security advisor from Public Safety Canada who can provide support and potentially alleviate some resource constraints.
- Leverage national communities of practice: larger, well-resourced member institutions can provide advice and guidance based on complex issues they may have faced.

- Engage with the provincial or regional communities of practice. Specific groups for the Pacific, Alberta, Quebec and other regions create additional forums for sharing best practices and getting regionally specific input.
- Leverage Government of Canada resources, including the safeguarding science workshops, training courses, etc.
- Look into consortium pricing on research security due diligence tools, and pool limited resources with other small to medium-sized institutions to access them.
- Leverage the advocacy of Universities Canada, which engages with the federal government on behalf of all universities regardless of size.

Day 1, Session #2: U15 and Large Universities

MAIN TAKEAWAYS

The decentralized structure of higher education institutions poses significant challenges to promoting awareness and implementing research security best practices and protocols.

There is a need for more resources, capacity, and support for research security teams from their respective institutions.

SUMMARY

The discussion centred around three prompts intended to provide a forum to address challenges unique to large institutions when delivering research security programs.

Wins

The first discussion prompt invited participants to share some of the research security wins from their institution and how they communicated this success. Participants shared that incorporating research security into mandatory training programs for staff and faculty had been successful as a form of risk mitigation and increasing familiarity with research security concepts. Some institutions cited the adoption of federal training courses as a success. However, some institutions shared that they had struggled to make research security training mandatory. The same participants noted that more support from institutional leadership is required to mandate training.

Decentralization

The second discussion prompt discussed the impacts of decentralization on managing research security requirements; many participants identified decentralization as one of the biggest challenges their research

security teams faced. Some participants were concerned about the ability to showcase the impact of their programs in the event of a review of their institution's research security efforts. While research security teams are often well-versed in how to share and enable research security best practices, there is no formalized process (e.g., program evaluations) to review the efficacy of these efforts and thus no way of measuring stakeholder aptitude in research security. A participant shared how their team tackles the decentralized nature of their institution by assigning each team member with responsibility for a research-intensive Faculty. Each team member can then build relationships with their assigned Faculties to integrate research security considerations and conversations both within and outside of grant application processes and cycles. The participant also noted that they have built-in redundancy, via a shared inbox, to ensure that there is always an easily accessible point of contact for researchers and staff navigating research security questions.

Scope of Work

The third prompt raised discussion about how, despite large universities being relatively well-resourced, research security teams are still limited in their capacity and asked how teams determine their purview. Many participants shared that they require more resources and capacity to properly address everything that is brought to them. A participant emphasized the importance of drawing boundaries to avoid "scope creep." Avoiding so-called scope creep is also essential to ensure requirements related to specific policies are completed carefully and to the highest standard. Participants briefly raised the potential to use artificial intelligence (AI) to help automate processes and increase efficiency. Strong validation methods still need to be developed before AI tools can become standard practice.

Day 1, Session #3: Research Hospitals, Institutes, and Non-Profits

MAIN TAKEAWAYS

- Research hospitals, institutes, and non-profits face ongoing challenges of promoting research security to researchers and explaining why research security matters.
- They also face resource challenges related to conducting training, purchasing due diligence tools and hiring qualified staff.
- Participants expressed a desire to balance national security (including research security) considerations while establishing a workable framework that does not stand in the way of innovation.

SUMMARY

Discussion included different organizations' approaches to adapting research security considerations to their contexts and how they differ from strictly academic institutions, as they may not have such a strong focus on federal research funding. As such, available support structures can vary widely. Some institutes have

researchers who hold positions at universities, and therefore, can submit grant applications via their assigned post-secondary institution. Such institutes, therefore, defer to universities to implement policies related to research security.

Institutes that have special contexts that inform their security posture, such as infectious disease labs, have an additional focus on the physical and cyber security aspects of the research security approach. The aim for these institutions is to take a more holistic approach to overall security, which also takes into account research-specific considerations for partnerships and collaborations.

Some institutes have adopted personnel-screening procedures by building relationships with teams that assist in the researcher hiring process. Building strong relationships with these other administrative teams helps raise awareness of research security requirements and appropriate screening practices.

Some institutes that also function as granting agencies have small teams to implement research security plans as required by the federal government. These institutes developed strong relationships with peer-institutes, including federal granting agencies, to share lessons and approaches to the effective implementation of the government policies. Some approaches include adapting the existing Tri-Agency guidance to create bespoke guidance for their institute. Institutes also shared the challenge of validating the risk assessments they receive, as there is a lack of guidance from the government on how to validate the information from a research security perspective.

Day 1, Session #4: Best Practices and Behavioural Insights from the United Kingdom

MAIN TAKEAWAYS

- The United Kingdom (UK) approaches research security from a trusted research and innovation perspective to consider all international partnerships and collaborative activities.
- The UK's Research Collaboration Advice Team (RCAT) supports and advises institutions on national security risks and helps them build capacity.

SUMMARY

To contextualize the discussion, the session began with an overview of the UK's research system and approaches to research security. The post-secondary sector is considered a critical component of the UK domestic economy, supporting approximately 250,000 jobs. The UK's ability to collaborate internationally is foundational to its success as a global leader in research and development.

Next, the different departments, as well as legislative and non-legislative measures that address research security issues, were discussed. The presenters emphasized that these measures are designed to be specific and proportionate to reduce the risk of unintended consequences, including a chilling effect on legitimate, valuable international collaborations. The measures include export controls, awareness campaigns and grant reforms. Additionally, the questions asked of applicants, as well as the risk assessment framework, were shared by the presenters.

The session then examined three case studies: a request for a scientific presentation abroad that included the presenter being approached by a foreign government for consultation, a university spin-off company seeking to commercialize its technology breakthrough, and the influence of institutional oversight on informal collaborations, particularly when they result in publications. Each case study was presented with a few questions for the attendees to consider, followed by small group discussions and a session-wide reflection.

Thirdly, the session discussed how to implement behavioural changes in support of research security. Researchers' limited time and attention due to competing demands–as well as the fact that research security requires constant vigilance–can negatively impact the implementation of efforts to support behavior change. To support change management, the UK recommends an "EAST" framework: make it "easy," make it "attractive," make it "social," and make it "timely."

Day 2, Session #1: Manual Open-Source Intelligence Approaches

MAIN TAKEAWAYS

- Open-source intelligence collection is grounded in traditional research methods, using context and experience with previous cases to drive a risk-informed approach.
- With limited resources, research security professionals have to balance their efforts with case requirements, based on their initial judgment of the case from experience and identifying key pieces of information for an assessment.

SUMMARY

To start the workshop, participants identified their common issues with manual approaches to open-source intelligence (OSINT) gathering. Participants wondered where to start their research, and raised questions relating to the tracing of searches to individuals or institutions, and "paywalled" materials; barriers relating to the translation of foreign-language materials were also highlighted.

Discussions included potential best practices for OSINT such as the use paid services and protecting one's identity when conducting due diligence work. Participants recognized that device and browser data communicated to websites can provide significant information about the user and the user's system, and emphasis was placed on practices to prevent the transfer of user data.

OSINT methodology is grounded in conventional research methods, using context and experience with previous cases to drive a risk-informed approach. Considering many research security teams work with limited resources, it was stated that a balance between effort and comprehensiveness of the assessment based on case needs is required. Emphasis was placed on context-driven approaches to searching. Throughout the session, several resources were mentioned, including Silo, Wayback Machine, the Organized Crime and Corruption Reporting Project (OCCRP) Aleph, and the Open Corporates Web Portal. These tools can help when conducting research while also protecting the user's identity and intellectual property.

Day 2, Session #2: Paid Platforms: Benefits, Downsides and Considerations

MAIN TAKEAWAYS

- Research security tools can save time, but using them is not absolutely necessary to effectively collect or analyze good-quality open-source intelligence (OSINT).
- There is value in "showing your work" when discussing risks with researchers. Tools can provide access to data or reports that can be shared during conversations about risk.
- Tools are expensive, and some institutions may instead opt to hire and train individuals to conduct open-source due diligence depending on their needs.
- Paid platforms don't provide "the whole truth;" fact-checking and/or follow-up is often required. While these tools can be useful in providing a starting point for analyses, research security professionals must also be able to understand how to analyze and contextualize the information provided by the tool.

Granting agencies and government departments can use tools to screen applications for concerns. As such, some feel the need to acquire tools to better conceptualize the concerns identified by the government or the granting agency.

SUMMARY

The goal of this session was to discuss considerations related to the acquisition and use of commercially available due diligence or research security-related tools (e.g., software, research platforms, etc.). Many participants in this discussion represented small-to-medium sized institutions and third-party organizations who are currently considering paid platforms that could improve their capacity for research security.

Additionally, several institutions that currently use paid platforms attended and shared their experiences, including feedback on client service, data fidelity, privacy concerns and the value of the paid platform. The discussions provided useful insights on paid platforms that will enable potential subscribers to make well-informed decisions in the context of limited budgets and resources.

Participants discussed the benefits and drawbacks of paid platforms, with an initial focus on sharing scenarios in which the tools may be helpful. Participants shared that tools can help reduce the time spent on complex open-source inquiries, including when certain searches require the review of several documents, websites or resources. Furthermore, some noted that tools may assist in collecting and analyzing data in languages other than English, thereby acting as a "force multiplier" for users who have limited time to conduct deep analysis of certain subjects.

Participants shared that the ease of use of particular platforms, as well as trust in the data, were important considerations in their decision to use a tool. In some cases, participants highlighted errors in the data generated by certain tools or confusion with the way the data is presented to users. Participants shared concerns about additional time spent verifying results from research security tools in the context of tight review timelines and limited team resources. One participant noted concerns about the increasing use of large language models to collect and structure data that is uploaded to platforms without adequate human verification or review.

Privacy was an additional consideration for some participants. Specifically, certain participants were concerned that some tools may store search data and/or other information on the platform. Depending on the jurisdiction in which a client operates the tool, the collection of user data may create privacy-related issues which need to be addressed by the tool vendor.

Day 2, Session #3: Public Safety Case Study and Workshop

MAIN TAKEAWAYS

- Participants learned of "red flag" indicators to consider when assessing internal risks and how existing institutional policies can strengthen research security, such as those involving intellectual property management, conflict of commitment, export controls, etc.

SUMMARY

The presenter led the group through a discussion to set the scene, where participants shared the types of risk assessments in place at their organizations, and the types of policies covering acceptable relationships amongst colleagues. Participants included representatives from small-to-medium-sized universities, public institutions and private organizations.

Next, participants were taken through a hypothetical case study where pieces of information were progressively disclosed. The participants were asked to assess the potential risks to the institution as the behaviour of a researcher and their postdoctoral fellow became increasingly erratic and inappropriate. By the end of the exercise, participants had successfully identified several warning indicators and potential consequences of the subjects' behaviours; they also discussed ways the outcome could have been prevented.

The session provided a productive discussion of different organizations' approaches to research security and risk mitigation and offered an opportunity to apply knowledge of research security practices to a case study.

Day 2, Session #4: Supply Chain and Procurement Considerations

MAIN TAKEAWAYS

- Cybercrime is the main threat facing supply chain and procurement processes, particularly financially motivated "Cybercrime-as-a-Service," and threats from the PRC, Russia, Iran, India, and the Democratic People's Republic of Korea.
- To mitigate the risks posed to supply chains, it is essential to incorporate security considerations in every step of the procurement process.

SUMMARY

This session discussed threat actors and motivations, threats to supply chains and how to assess them, and how to build security into the procurement process.

Threat Actors and Motivations

Canada's state adversaries are using targeted misinformation campaigns to disrupt and divide the voting population's political opinions. The primary adversaries are the PRC, Russia and Iran, followed by the Democratic People's Republic of Korea and India. Ransomware is the top cybercrime threat to Canada's infrastructure. There has been an increase in Cybercrime-as-a-Service (CaaS) whereby individuals or firms are hired to commit cybercrime against other individuals or organizations. This type of financially motivated cybercrime is the cyber threat activity most likely to affect Canadian citizens, residents and organizations.

Supply Chain Threats

Supply chain threats are more complex than direct compromises to an institution's research security and are likely to remain a tool for state-sponsored threat actors and advanced cybercriminals. Supply chain threats involve the indirect exploitation of targets via vulnerabilities in supply chains and internet infrastructure. This kind of threat is becoming increasingly common as cloud-based software and infrastructure becomes ubiquitous. There are three types of supply chain compromises: software, hardware, and the use of third-party networks to gain access. To manage supply chain threats, research institutions need to identify, assess, mitigate, and monitor their risk concerns.

Building Security into the Procurement Process

Some essential principles to strive for include: implementing security in every step of the procurement process, trusting attestations while still seeking validation, establishing robust risk assessment and mitigation processes, and establishing good governance, such as early engagement and ongoing monitoring.

CONCLUSION AND LOOKING AHEAD

The 2025 Research Security Conference took place at a critical juncture for the research security community. Given the speed at which the Canadian community of dedicated research security professionals has grown, this was the first opportunity for many colleagues to meet in person. Participants discussed how best to support researchers in both promoting security and openness in their work amidst a growing range of regional, national and international research security frameworks.

The event made clear that research security in Canada has evolved significantly in a very short period and that federal investments in Canadian institutions to support their research security efforts have yielded significant returns.

Communities of practice—such as the Team Canada research security network—were repeatedly identified as valuable mechanisms for building shared resiliency and competencies. As international counterparts continue to develop their frameworks for research security, it will be important to seek opportunities for alignment across these new paradigms whenever possible.

By the event's conclusion, it was clear that in addition to adequately safeguarding research, stakeholders also need to invest in and support the research they are trying to protect. The consequences of overcorrection and the potential for the loss of talent or for limiting the risk of partnerships cannot be overstated. Research security professionals must be aware of the human impacts of overly strict or erroneous application of research security frameworks. It will be critical for government entities developing and enforcing requirements to continue open communication and dialogue with those who conduct and facilitate research. Enabled by critical government support, continued engagement with higher education institutions is integral to creating a safe and open Canadian research ecosystem.

Looking Ahead: 2026 Research Security Conference

The 2026 Research Security Conference will be co-hosted by the University of Manitoba and the Toronto Metropolitan University. The conference is tentatively scheduled to take place in May 2026 in Winnipeg, Manitoba.

The team at the University of British Columbia is grateful to have hosted the 2025 Research Security Conference and thanks those who contributed to making the 2025 conference in Vancouver a reality.

We look forward to next year's conference and continuing to collaborate in support of a Canadian research ecosystem that remains as open as possible and as secure as necessary.

The University of British Columbia acknowledges the Government of Canada's Research Support Fund for its role in enhancing and promoting research security and in developing and sustaining an environment to support research and scholarly excellence.