College and Institute Applied Research in a Safe Innovation Ecosystem

Submitted to Public Safety Canada

July 2021
Colleges and Institutes Canada (CICan) is the voice of Canada’s publicly-supported colleges, institutes, cegeps and polytechnics, and an international leader in education for employment with ongoing programs in over 25 countries.

CICan’s members add over $190B to Canada’s economy each year and contribute to inclusive economic growth by working with industry and community partners to offer more than 10,000 programs to learners in urban, rural, remote, and northern communities.
College and Institute Applied Research in a Safe Innovation Ecosystem

Submission to the Government of Canada consultation on Economic Threats to National Security

Recommendations:
1) That the federal government continue to invest in tools and resources to create a more cyber secure research environment for colleges and their innovation partners
2) That the federal government coordinate with all levels of government to align on a common set of national guidelines for ensuring research security, and that this effort be supported by a mechanism that can be adopted by all research stakeholders.
3) That the federal government provide specific and ongoing training through college applied research offices to equip researchers, students, SMEs and community innovation partners with the knowledge and skills they need to create and maintain a safe research environment.
Applied Research at Colleges and Institutes

The primary mission of colleges and institutes is to provide accessible, high-quality education and skilled workforce development that is responsive to local and regional economies. Over 95% of Canadians live within 50 km of a college campus, community learning centre or applied research facility. As part of their close link with industry and community partners, colleges serve as local gateways to the innovation ecosystem for thousands of small and medium enterprises (SMEs) and other organizations every year, specializing in research that solves technology, business and other innovation challenges. In 2019-2020, they reported over 8,000 research partnerships, the vast majority of them with SMEs, who often lack the resources, specialized technology and networks to solve innovation challenges on their own. Colleges develop the talent employers need and provide the expertise required to develop or improve products, processes and services and enhance their partners’ competitiveness, efficiency and sustainability. Some 42,000 students participated in applied research activities in 2019-2020, gaining valuable work-integrated learning (WIL) experience. Partnered applied research solves innovation challenges at the “speed of business”: In 2019-2020, applied research offices reported over 5,500 new processes, products, prototypes and services, 85% of which were completed in under one year.

The applied research ecosystem is jointly funded by federal and provincial research grants as well as substantial private sector contributions and key investments made by colleges themselves. It has expanded considerably in recent years as industry and other innovation partners see the value in collaborating with college resources and expertise to solve practical challenges. Applied research receives a total of $345M in annual funding from all sources, which represents a 19% growth over two years. Private sector contributions have increased by 42% over the past two years, and now match dollar-for-dollar with federal government investments. Similarly, the number of students participating in applied research activities has grown by 45% over the past two years. Applied research contributes to innovation in both well-established economic sectors such as agriculture, manufacturing, health and social services, as well as emerging areas of high growth for Canada, including biomanufacturing, quantum technology, artificial intelligence and genomics. Nevertheless, only 2% of the total annual federal spending on research is allocated to supporting college applied research.

Economic-based threats to national security in the context of partnered applied research

The problem of foreign hostile state and non-state actors seeking to acquire technologies or enter into commercial partnerships that can potentially put at risk Canada’s national security and long-term economic prosperity is of serious concern and affects all parts of the innovation and research ecosystem, including college applied research. In recent years, many Canadian companies, in almost all sectors of the economy, have been targeted, compromised and have suffered losses from human and cyber enabled threats. Colleges themselves have not been immune, and several recent high-profile incidents of cyber attacks on institutions have been well-publicized. This problem is by no means unique to Canada, and each of our Five Eyes partner countries (United States, United Kingdom, Australia and New Zealand) is actively engaged in implementing resources and guidelines to safeguard research and innovation in

---

1 References to “colleges” refer collectively to publicly-assisted colleges, institutes, polytechnics, cégeps.
2 All data from Colleges and Institutes Canada’s 2019-2020 member survey on applied research.
higher education. This presents Canada with an opportunity to learn from others and adopt best practices as it seeks to create its own national strategy for research security.

In working with various partners in the research ecosystem, the Government of Canada is continuously developing measures to protect sensitive and emerging goods and technologies, critical infrastructure, and sensitive personal information from espionage, theft and cyber attacks. Through their partnerships with thousands of SMEs and community organizations, colleges play an important role in developing and implementing this strategy.

In addressing economic-based threats to national security, it is important to highlight several ways in which college-based applied research differs from university-based discovery research:

- Applied research is partner-driven. The intellectual property (IP) always remains with the industry partner or client – colleges do not commercialize any research themselves and do not hold IP rights in the vast majority of cases.
- Most of the time the same holds true for pre-commercial research data – this also resides on the infrastructure and IT systems of the industry partner or client, and not with the college itself.
- Interactions with industry partners and other clients are frequent and short in duration: most research results are developed in less than a year.
- The applied research partners are small (most are SMEs) and are not typically resourced to undertake research activities and accompanying responsibilities (such as research security) on their own.
- By-and-large, colleges are not eligible for research capacity support, such as the Research Support Fund administered by the Tri-Agency programs (NSERC, SSHRC, CIHR). Federally administered college applied research grants typically allow for some overhead costs, but only to the particular project covered by the grant. This lack of institution-specific, capacity-building resources makes it more challenging for colleges to develop and implement underlying, broad-based initiatives such as research data management (RDM), ensuring research integrity, meeting regulatory and ethical standards, administrative support, and research security.

The result is that while colleges and the SMEs they partner with are less likely to be targeted for attacks due to their smaller profile and focus on applied, non-fundamental research, they nevertheless remain extremely vulnerable to threats due to capacity and resource constraints. Although the industry clients working with colleges are perhaps less of an “obvious target” than critical utilities infrastructure or some of the “well known” national laboratories and research centres housed at universities, they play an important role in the broader supply chain that supports key industries such as biomanufacturing and AI where IP and other assets might be stolen. The typical SME is even less capable than a college itself in guarding against cyber threats, and since research data and IP resides with the industry client, the risk profile can be quite broad.

Current trends indicate that both government direction towards commercialization of research and the real value proposition college-based applied research brings to business and other innovation partners will only accelerate the growth of this portfolio. It is key to put systems and structures in place now to safeguard it.
Proposed solutions and strategies

To safeguard against economic-based threats to national security as they relate to college applied research, we encourage the federal government to equip college applied research offices and their innovation partners with appropriate resources, guidelines and training.

1) Resources

Because colleges lack access to dedicated research support funding, it is more challenging for them to properly implement research security measures. Offering a single, centralized approach to research security amongst all government departments and stakeholders will ensure that requirements and standards are easier to adopt and implement across a variety of research activities. These resources could include specific tools or software to help mitigate the threats posed by cyber crime, such as an automated process (perhaps powered by AI) to assist all institutions and researchers in carrying out due diligence without having to become experts in particular aspects of research security.

Current resources in development such as the Safeguarding Your Research portal are well appreciated but at this time are not widely known within the college community. More effort is needed to promote the current suite of tools and ensure that they are adapted to the realities of partnered applied research with SMEs. By leveraging the collaboration that colleges enjoy with their innovation partners, the government has an opportunity to make safe research tools and practices more widely available to a broader audience and indeed Canadian society at large.

- Recommendation: That the federal government continue to invest in tools and resources to create a more cyber secure research environment for colleges and their innovation partners

2) Guidelines and Mechanisms

It is critical that governments of all levels (federal/provincial/municipal) align on requirements for research security and its implementation. Existing research mechanisms such as the Tri-Agency Framework on the Responsible Conduct of Research (RCR) or Research Ethics Boards (REB) are not specifically equipped to deal with cyber security and economic-based threats to national security. Mechanisms such as the Controlled Goods Program are better suited to provide guidance and leadership in developing guidelines for research security, particularly in the context of applied research, where the research results are tangible and products and services in various stages of commercialization.

Because the college applied research community is not generally equipped to develop its own guidelines surrounding research security, colleges would appreciate guidance from the federal government and awareness of key risk areas of concern. Coupled with the appropriate tools, this endeavour could ensure colleges and their research partners are continuously aware of the evolving threat landscape.

A one-stop shop approach is needed to streamline the recent initiatives undertaken by the federal government in promoting research security, and directives should be communicated clearly to applied research offices as well as the Chief Information Officers at colleges. National associations such as Colleges and Institutes Canada can play an important role in facilitating this collaboration.
• **Recommendation:** That the federal government coordinate with all levels of government to align on a common set of national guidelines for ensuring research security, and that this effort be supported by a mechanism that can be adopted by all research stakeholders.

This kind of approach to safeguarding research in an academic and partner-driven context has been adopted by other countries (notably, each of the Five Eyes partners) and Canada could do well to study what has worked successfully and perhaps adopt best practices.

3) **Training**

Resources and guidelines cannot be implemented effectively without proper training. Because college applied research operates on a grant-to-grant basis, with a rapidly changing roster of innovation partners, everyone in the ecosystem needs to be equipped with basic tools to ensure research security. Current training capacity for broad-based research support services such as research security is very limited in the college system. Colleges would benefit from a regular program of briefings on topics such as actors who are actively targeting Canadian researchers, how to do effective background checks, tailored advice on cyber security, and suggestions about contractual arrangements to limit access to or prevent theft of sensitive research.

• **Recommendation:** That the federal government provide specific and ongoing training through college applied research offices to equip researchers, students, SMEs and community innovation partners with the knowledge and skills they need to create and maintain a safe research environment.

**Conclusion**

Colleges across the country play a lead role in Canadian innovation and prosperity by partnering with industry (particularly SMEs), and community organizations to engage in applied research that enhances their partners’ competitiveness, efficiency, and sustainability. With over 400 specialized research centres and laboratories, colleges and their students work with partners in all sectors to develop or refine solutions, products, services, technologies, and processes. Like all sectors of the wider research ecosystem, colleges and their innovation partners are vulnerable to cyber attacks, IP theft, and other economic based threats to national security. We encourage the federal government to help create and maintain a safe applied research environment by supporting colleges with appropriate resources, guidelines and training opportunities. By leveraging the research partnerships colleges create with industry and community organizations, these investments can play a key role in creating a more cyber secure Canada.
CICan Member Colleges and Institutes in Canada

Over 95% of Canadians live within 50 km of a college or institute.

This extensive network of post-secondary institutions serves students from all over the country where they live, whether it’s in urban, rural, northern or remote communities, thanks to more than 680 campuses or facilities across Canada.
CICan Member Colleges and Institutes in Canada

Yukon
- Yukon University

Northwest Territories
- Aurora College
- Collège Nordique Francophone

Nunavut
- Nunavut Arctic College

British Columbia
- British Columbia Institute of Technology (BCIT)
- Camosun College
- Capilano University
- Collège Educentre
- College of New Caledonia
- College of the Rockies
- Douglas College
- Justice Institute of British Columbia
- Kwantlen Polytechnic University
- Langara College
- Native Education College
- Nicola Valley Institute of Technology (NVIT)
- North Island College
- Northern Lights College
- Coast Mountain College
- Okanagan College
- Selkirk College
- Thompson Rivers University
- University of the Fraser Valley
- Vancouver Community College
- Vancouver Island University (VIU)

Alberta
- Bow Valley College
- Centre collégial de l’Alberta
- Grande Prairie Regional College (GPRC)
- Keyano College
- Lakeland College
- Lethbridge College
- Medicine Hat College
- NorQuest College
- Northern Alberta Institute of Technology (NAIT)
- Northern Lakes College
- Olds College
- Portage College
- Red Deer College
- SAIT

Saskatchewan
- Carlton Trail College
- Collège Mathieu
- Cumberland College
- Dumont Technical Institute
- Great Plains College
- North West College
- Northlands College
- Parkland College
- Saskatchewan Indian Institute of Technologies
- Saskatchewan Polytechnic
- Southeast College

Manitoba
- Assiniboine Community College
- École technique et professionnelle, Université de Saint-Boniface
- Red River College
- University College of the North
- Manitoba Institute of Trades and Technology

Ontario
- Algongquin College
- Cambrian College
- Canadore College
- Centennial College
- Collège Boréal
- Conestoga College Institute of Technology and Advanced Learning
- Confederation College
- Durham College
- Fanshawe College
- First Nations Technical Institute
- Fleming College
- George Brown College
- Georgian College
- Humber College Institute of Technology & Advanced Learning
- Kenjgewin Teg Educational Institute (or KTEI)
- La Cité
- Lambton College
- Loyalist College
- The Michener Institute of Education at UHN
- Mohawk College
- Niagara College
- Northern College
- Sault College
- Seneca College
- Sheridan College
- Six Nations Polytechnic
- St. Clair College
- St. Lawrence College

Quebec
- Collège André-Laurendeau
- Collège de Chicoutimi
- Le cégep de Granby
- Collège de Jonquière
- Collège de l’Abitibi-Témiscamingue
- Collège de la Gaspésie et des Îles
- Collège de La Pocatière
- Collège de Matane
- Collège de Rimouski
- Collège de Saint-Félicien
- Collège de Sainte-Foy
- Collège de Saint-Hyacinthe
- Collège de Saint-Jérôme
- Collège de Saint-Laurent
- Collège de Sept-Îles
- Collège de Sherbrooke
- Collège de Trois-Rivières
- Collège de Victoriaville
- Collège du Vieux Montréal
- Collège Édouard-Montpetit
- Collège Garneau
- Collège Limolou
- Collège Marie-Victorin
- Collège régional de Lanaudière
- Collège Rivièvre du Loup
- Collège Saint-Jean-sur-Richelieu
- Champlain Regional College
- Collège Ahuntsic
- Collège André-Grasset
- Collège d’Alma
- Collège de Bois-de-Boulogne
- Collège de Maisonneuve
- Collège de Rosemont
- Collège LaSalle
- Collège Mérici
- Collège Montmorency
- Collège Shawinigan
- Collège de Saint-Boniface
- Université de Montréal
- Université de Sherbrooke
- Université de Sept-Îles
- Université de Saint-Laurent
- Université de Saint-Jérôme
- Université de Sainte-Foy
- Université de Rimouski
- Université de Matane
- Université de la Gaspésie et des Îles
- Collège de l’Abitibi-Témiscamingue
- Le cégep de Granby
- École technique et professionnelle, Université de Saint-Boniface
- École technique et professionnelle, Université de Montréal
- École technique et professionnelle, Université de Sherbrooke
- École technique et professionnelle, Université de Sept-Îles
- École technique et professionnelle, Université de Saint-Laurent
- École technique et professionnelle, Université de Saint-Jérôme
- École technique et professionnelle, Université de Sainte-Foy
- École technique et professionnelle, Université de Rimouski
- École technique et professionnelle, Université de Matane
- École technique et professionnelle, Université de la Gaspésie et des Îles

Associates
- Association des collèges privés du Québec
- Association québécoise de pédagogie collégiale
- Atlantic Provinces Community College Consortium (APCCC)
- BC Colleges (BCC)
- Canadian Association of Diploma and Technology Colleges (CADAP)
- Colleges Ontario
- Council of Postsecondary Presidents of Alberta (COPPOA)
- Fédération des cégeps
- Forum for International Trade Training (FITT)
- Horatio Alger Association of Canada
- Inter-American Organization for Higher Education (IOHE)
- Regroupement des collèges du Montréal métropolitain (RCMM)
- Synchronex
- Tra Vinh University

Please refer to our website for the most updated information:
collegesinstitutes.ca/members