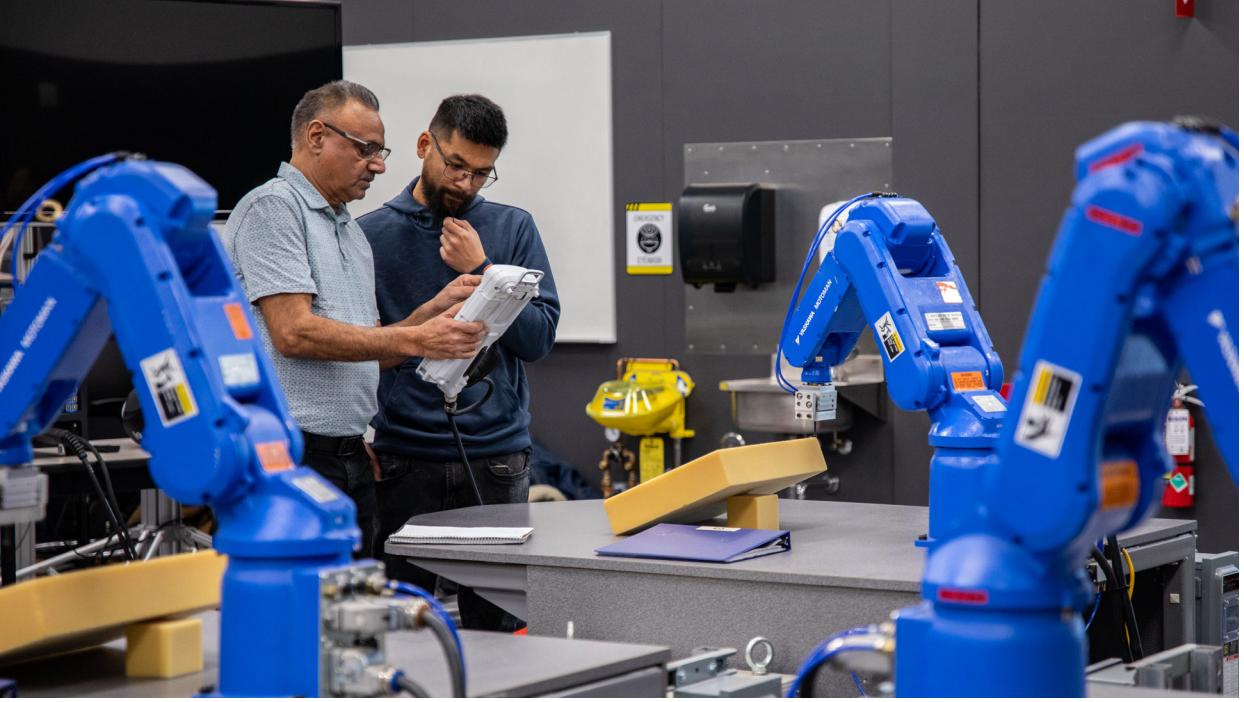
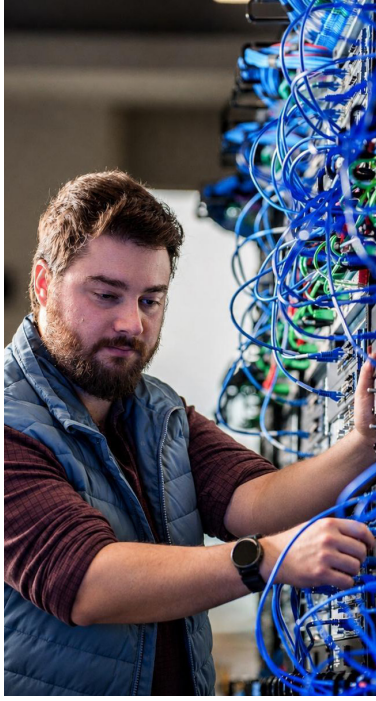




Risks and Threats to Canadian Science and Research

SUBMISSION TO THE HOUSE OF COMMONS STANDING COMMITTEE ON SCIENCE AND RESEARCH

POLYTECHNICSCANADA





November 2026

POLYTECHNICSCANADA

Recommendations

- Establish dedicated research security funding for polytechnics and colleges
  Costs associated with safeguarding industry-driven applied research, including projects supported by businesses and funded under the College and Community Innovation Program, do not qualify for existing federal research security funding.

- Develop research security protocols proportionate to risk
  Risk assessment, due diligence and reporting requirements must account for industry-led collaborations, the prevalence of small- and medium-sized businesses (SMBs), and the need to protect commercially sensitive information without creating undue barriers.

- Support institutional cybersecurity readiness and secure research infrastructure
  To fully participate in sensitive and defence-related research, institutions require secure data environments, information management systems, facility upgrades and capacity to meet enhanced security requirements.

- Build research security capacity across the broader innovation ecosystem
  Specialized initiatives such as Defence Innovation Secure Hubs (DISHs) must be paired with investments that enable polytechnic facilities to undertake sensitive research securely, connect with specialized hubs and contribute to Canada's strategic innovation priorities.

POLYTECHNICSCANADA

Context

Canada's science and research ecosystem is operating in an increasingly complex threat environment. The research security risks associated with intellectual property, sensitive technologies and confidential information are top of mind at polytechnics that undertake industry-led applied research activities in support of Canadian business innovation.

The Canadian Centre for Cyber Security's National Cyber Threat Assessment 2025–2026 identifies intellectual property theft and cyber espionage among the threats facing Canadian organizations. It warns that state-sponsored actors target proprietary information to advance economic and military interests, including those associated with strategically important and emerging technologies. These risks extend beyond fundamental research of the kind carried out at universities to the collaborations through which Canadian businesses develop, validate and commercialize products and services.

This latter type of research – designed to help business partners solve technical challenges, develop products, test emerging technologies and bring innovations to market – is where polytechnics operate as innovation intermediaries. Unlike research models that develop and retain intellectual property, polytechnic applied research leaves IP where it stands to generate the greatest economic impact – with industry itself.

The scale of these activities is significant. In 2025–26, Polytechnics Canada's 13 member institutions:

- Undertook 4,166 applied research projects involving 2,825 partners
- Co-developed 1,206 prototypes, helping partners generate new capabilities
- Engaged 16,275 students, building an innovation-ready talent pipeline
- Deployed more than $42 million in federal research funding and leveraged another $72.2 million from other sources

As Canada seeks to secure sovereign capabilities, the support provided by polytechnics is increasingly aligned with national ambitions and priorities. Polytechnics help partners explore dual-use applications, adopt artificial intelligence and expand international markets. They derisk technology adoption and find solutions to drive productivity and competitiveness. Secure environments and institutional threat readiness is more important than ever.

Yet, polytechnic institutions and colleges cannot access current federal supports related to research security. The Research Support Fund's dedicated research security component requires institutions to receive at least $2 million annually in research funding from a limited number of eligible programs. Polytechnic applied research, much of which is conducted in a program deemed ineligible for the Research Support Fund, receives no research security support.

This stands to sideline important contributors to Canada's research ecosystem as their brand of research becomes increasingly critical. To safeguard commercially and strategically sensitive research, uneven funding must be addressed.

Protecting Canadian IP in Applied Research

Research security at polytechnics is closely connected to the protection of commercially sensitive information and intellectual property belonging to Canadian businesses.

Applied research partnerships frequently require companies to share proprietary designs, manufacturing processes, technical specifications, software, datasets and other confidential information. Because industry partners retain ownership of IP generated during these projects, polytechnics serve as trusted custodians of valuable business information. Protecting that information is essential to preserving commercial value beyond the life of the project, requiring institutions to assess and plan for risk associated with unauthorized access, cyber incidents, insecure information transfers or inappropriate disclosure.

At the same time, applied research operates differently from traditional academic research activities. Projects are often short-term, developed in response to immediate business needs and undertaken with companies that have limited internal research capacity. Businesses rely on polytechnics precisely because they offer accessible expertise and infrastructure that would otherwise be difficult or expensive to obtain.

Research security requirements must, therefore, account for both the information being protected and the operating environment in which the research takes place. Applying the same administrative processes to every partnership, regardless of its sensitivity or risk profile, stands to create an unnecessary burden for institutions and smaller businesses, delaying projects without necessarily improving security outcomes.

A proportionate approach would allow institutions to assess risk according to the sensitivity of the technology and information involved, the nature of the partnership and the potential consequences of unauthorized access or disclosure. This requires practical assessment tools, clear guidance and sufficient institutional expertise to implement appropriate safeguards efficiently. The objective should be to strengthen the protection of Canadian business IP while preserving the accessibility and responsiveness that make industry-driven applied research valuable.

Growing Security Expectations Are Outpacing Institutional Capacity

While research security policies have placed greater emphasis on identifying and mitigating risks, effective implementation depends on stable institutional resources.

Institutions need personnel who can assess sensitive research activities, advise researchers and industry partners, develop security procedures and oversee compliance. They also require appropriate cybersecurity systems, secure data environments and information management infrastructure to protect confidential information. These are ongoing institutional responsibilities beyond the scope of research project budgets.

The practical consequences are already apparent in applied research collaborations. An AI-enabled quality inspection project involving an aerospace manufacturer, for example, has encountered delays because researchers require access to sensitive product conformity images maintained within the company's internal network. The information cannot be transferred through conventional cloud services or portable storage devices under the company's security requirements. Although the technical expertise to develop and validate the technology is available, the lack of an appropriate secure research environment complicates access to the data needed to undertake the work.

This illustrates how insufficient security infrastructure can constrain legitimate innovation. A trusted research environment with appropriate access controls and data management safeguards could enable the collaboration while protecting proprietary manufacturing information and meeting the partner's security expectations.

Similar considerations arise in defence-related applied research that involves sensitive information about individuals. For instance, developing and validating a digital support tool intended for military personnel and veterans may require enhanced confidentiality and privacy safeguards, particularly where personal information could be involved in testing or evaluation.

Expanding institutional research security funding to reflect the full scope of applied research activity would help address this gap. Such support should recognize research security as an ongoing institutional function, enabling polytechnics to establish the expertise, systems and infrastructure necessary to protect Canadian businesses and undertake sensitive research.

Building Research Security Across the Innovation Ecosystem

Canada's growing emphasis on defence innovation and sovereign technological capabilities makes institutional research security capacity increasingly important. DISHs provide secure, mission-oriented research environments intended to bring together government, industry and research partners to develop, test and validate technologies relevant to national security.

The DISH program also illustrates a broader challenge related to institutional research security readiness. Applicants are required to submit a research security plan outlining potential risks, mitigation measures, protection of sensitive information and security governance arrangements. For polytechnics without established research security capacity or dedicated funding to develop it,

these requirements can represent a barrier to preparing competitive proposals, even when institutions possess relevant technical expertise, facilities and industry relationships. This highlights an important gap in Canada's ability to activate the entirety of its research ecosystem to achieve national priorities.

DISHs themselves respond to a recognized infrastructure challenge. The Department of National Defence's 2026 DISH Applicant Guide acknowledges that establishing and operating secure research environments capable of accreditation up to Level II (Secret) is complex and resource-intensive, often exceeding the capacity of individual organizations. The program accordingly supports modifications to existing infrastructure to enable secure defence research. However, specialized hubs cannot address the full range of research security needs across Canada's innovation ecosystem.

Polytechnics already operate research facilities and laboratories in areas relevant to national security, including aerospace, advanced manufacturing, artificial intelligence, robotics and digital technologies. Many industry collaborations involving these capabilities require secure data handling, cybersecurity safeguards or other protections without necessarily requiring classified facilities or falling within a specialized defence hub's mandate.

Investing exclusively in a limited number of secure environments stands to leave a broader need for institutional security unaddressed. It could also limit Canada's ability to mobilize existing applied research facilities and expertise.

A more effective approach would complement specialized secure hubs with targeted investments across the wider applied research ecosystem. This would enable institutions to strengthen baseline research security, upgrade existing infrastructure and undertake appropriately secured projects, while accessing specialized facilities when activities require higher levels of protection. This would make more effective use of existing public investments in research infrastructure, expand participation by Canadian businesses and strengthen pathways between applied research and defence innovation.

Strengthening research security across Canada's polytechnics would protect the intellectual property of Canadian businesses, enable more trusted research partnerships and ensure existing applied research expertise and infrastructure can contribute to Canada's national security, economic competitiveness and technological sovereignty.

POLYTECHNICSCANADA

About

Polytechnics Canada is the voice of leading research-intensive, publicly supported polytechnics and institutes of technology. We advocate for federal action in areas where polytechnics provide solutions for a more innovative, productive and globally competitive country. Polytechnics Canada members play a critical role in addressing some of the country's greatest challenges. Through their facilities and networks, our members provide meaningful solutions to industry problems and accelerate knowledge transfer.

ALGONQUIN COLLEGE

BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

CONESTOGA Connect Life and Learning

FANSHAWE

GEORGE BROWN POLYTECHNIC

HUMBER POLYTECHNIC

KPU KWANTLEN POLYTECHNIC UNIVERSITY

NAIT

RRC POLYTECH

SAIT

SASKATCHEWAN POLYTECHNIC

Seneca POLYTECHNIC

Sheridan