National

**Quantum Strategy**

# Securing Canadian Quantum Research and Development

Government of Canada | Gouvernement du Canada

Canada

This publication is available online at https://ised-isde.canada.ca/site/national-quantum-strategy/en/securing-canadian-quantum-research-and-development

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/publication-request or contact:

ISED Citizen Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON  K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ised-isde@ISED-ISDE.gc.ca



Cat. No. Iu37-50/2024E-PDF
ISBN 978-0-660-74037-9

Aussi offert en français sous le titre *Assurer la sécurité de la recherche et du développement dans le domaine quantique canadien*

# Introduction[1]

The Government of Canada aims to capitalize on the economic and defense potential of quantum technologies through the *National Quantum Strategy* (NQS) and the *DND/CAF's Quantum Science and Technology Strategy* and corresponding implementation plan, *Quantum 2030*. At the same time, there is growing awareness of significant security risks, especially in areas with potential military applications (i.e. dual-use technologies). Risks include potential theft, misuse or exploitation of knowledge and assets by bad actors to the detriment of researchers, businesses and the Canadian economy and society. In response, the Government has implemented export controls for certain technologies related to quantum computing.[2] Following the Policy on Sensitive Technology Research and Affiliations of Concern, safeguards have also been created to prevent federally-funded research in sensitive technology areas from being undertaken by researchers "connected to military, national defence, or state security entities that could pose a risk to Canada's national security." Sensitive technology research areas include quantum science and technology, specifically communications, computing, materials, sensing and software. In addition, the Government has launched the Research Security Centre and Safeguarding Your Research portal to provide guidance on protecting research and intellectual property.

This document intends to increase awareness about security risks and mitigation measures for Canadian universities, colleges, and businesses conducting quantum research and development (R&D). It also provides links to relevant Government of Canada policies and regulations, programs, resources, and contacts. It was developed by Innovation, Science and Economic Development (ISED)'s NQS Secretariat, in consultation with Public Services and Procurement Canada (PSPC), Public Safety Canada (PSC), the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (the Cyber Centre), the Department of National Defence (DND), the Canadian Security Intelligence Service (CSIS), and the Royal Canadian Mounted Police (RCMP).

There are several benefits to enhancing the security of quantum R&D facilities. Protecting assets and the commercialization potential of research ensures that the ones directly involved in the work benefit fully from it. Safeguarding the rewards of innovation also incentivizes further breakthroughs. The integrity and reputation of the Canadian quantum sector would be at risk if its research results and technologies were exploited for unintended, unethical and harmful ends, such as mass surveillance or violation of human rights. Preventing such misuse protects the sector's reputation, maintains social trust, and encourages widespread adoption. Also, organizations collaborating with the Canadian government or other security organizations (e.g. NATO) on defense-related research need to demonstrate that classified information and assets will be well-protected. Taking proactive actions to enhance security can help speed up contracting processes.

Improving organizational security requires proactive leadership and a clear accountability structure. Larger organizations may consider appointing a chief security officer to coordinate and oversee all security management activities. While having a full time security officer may be unrealistic for smaller organizations and start-ups, they could potentially engage a security consultant, and would still benefit from reviewing the resources presented in this document, increasing their understanding of security risks, and implementing whatever mitigation measures are relevant to their circumstances.

[1] Version 1 - 20 September 2024
This document is updated regularly. Please consult the website for the most up to date information.
[2] Notice to exporters No.1129 - Amendment to the Export Control List: Quantum computing and advanced semiconductors

# Common security threats and mitigation measures

The following is an overview of common security risks and mitigation measures for organizations involved in quantum technology R&D. For more detailed information on best practices, please consult PSPC's Contract Security Manual[3] and ISED's Research Security Training Courses. The Guidance for Research Organizations and Funders on Developing a Research Security Plan also provides information at the organizational level.

Threats can come from bad actors (state and non-state), as individuals or groups, from both inside and outside an organization. **Insider threats** include anyone who has knowledge of, or access to, an organization's assets and who could inadvertently or knowingly exploit this access for illegitimate purposes. **Outsider threats** encompass individuals or groups that do not have authorized access to an organization's assets, but who act in a way that could lead to the illegitimate acquisition of assets and subsequent harm. The most common vectors through which bad actors can pose a **security threat** include:

- people
- partnerships
- physical access
- cyber breaches
- intellectual property sharing

While this document is primarily intended for organizations, researchers should also consider relevant risks and mitigation measures especially related to work that could have adverse ethical or national security implications. While publication of research results and open science are valuable, such openness comes with associated risks to privacy, research outcomes, intellectual property, national security and the public interest. Even in cases where the research is intended to be published, unwanted transfer of knowledge can occur, potentially leading to a researcher's work being misused, corrupted, or distributed in ways or on timelines they have not agreed to. As well, the underlying data may not be included in a publication, but can still be valuable for potential future use. As a result, openness should be maintained to the maximum extent while acknowledging the need for safeguards in the case of research that could have adverse implications for researchers, national security or the public interest.

> Foreign actor interference, or suspicion of such activities, should be reported to the RCMP's National Security Information Network at 1-800-420-5805 or at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca; or to the local police. Suspicious activity or behaviour that has a connection to national security or may indicate serious criminal activity can be reported to the RCMP's National Critical Infrastructure Team (NCIT) at SIR-SIS@rcmp-grc.gc.ca.

[3] PSPC's Contract Security Program only provides services in the context of government contracts. However, organizations may consult the Contract Security Manual as a reference document on best practices to be applied on a voluntary basis to their own facilities and processes.

# Risks related to people

Some parties may seek to exploit direct or indirect access to an organization's personnel in order to access its R&D assets. This could be done for many reasons, such as to serve these parties' own agendas, competing commercial interests, or the interests of a foreign power. Personnel who are lax in observing security measures or accidentally leak information are also an unwitting threat.

**Mitigation measures include:**

- implementing security screening protocols and reference checks before hiring personnel,[4] as well as ongoing suitability and reliability procedures, and periodic audits
- ensuring that security screening and background checks include all relevant personnel such as: employees, vendors, contractors and staff
- implementing a process for declaring conflicts of interest and using non-disclosure and confidentiality agreements
- implementing security awareness and training requirements for employees
- implementing internal procedures for reporting suspicious activities or behaviours associated with insider risk

# Risks related to partnerships and collaborations

Collaboration and partnership-building are important to advance quantum technologies. While these arrangements can be successful, they can also be exploited by bad-faith actors who obscure their intentions, commitments or affiliations to advance goals that do not align with their partner's objectives and values.

**Mitigation measures include:**

- consulting the government's list of Named Research Organizations that are known to have foreign military ties or affiliations which may pose a risk to Canada's national security
- using the National Security Guidelines for Research Partnerships, the associated risk assessment form and the CSIS – Safeguarding your research checklist to evaluate the risk involved in partnerships and engagement with foreign organizations (research, commercial, non-profit) or individuals
- being aware of foreign ownership, control, or influence so that third parties do not exert influence over a Canadian organization to access classified information and assets
- ensuring that foreign and domestic partners fully disclose any potential conflicts of interest; in case of doubt, performing an open source search to see if a potential partner has been involved in questionable activities; if still unclear, re-considering the partnership

[4] Organizations may consult the Standards on Security Screening employed by the Government of Canada for guidance.

# Risks related to physical access

Facilities where quantum R&D is undertaken and where work is stored can be targeted to gain access to sensitive data, information and knowledge. Individuals may try to steal research, for example, by observing sensitive information or installations, taking pictures of lab facilities, equipment or notes, or using fake credentials to access restricted areas.

**Mitigation measures include:**

- establishing an overall security plan for the organization/facility
- establishing physical security zones as part of a security plan and developing policies on the storage and management of information and assets in the appropriate security zones, and communicating those plans to management and staff
- ensuring proper entry controls to access security zones (e.g. established entry points, escorting visitors, personnel IDs, electronic access control, locking up electronic devices prior to entry)
- ensuring security zones have proper CCTV and Intrusion Detection System monitoring and coverage
- for larger organizations, ensuring there is a security force to guard the facility and that they have proper patrol or post orders covering the security zones
- ensuring visibility into security zones is limited from the street or neighbouring buildings
- controlling access to sensitive information in a registry and segregating information so that it can only be accessed by individuals with a need to know
- marking, securing storage and transmission of, and properly destroying sensitive information in non-electronic format
- safeguarding research and related assets (e.g. prototypes, laptops, etc.) when personnel are travelling, both inside and outside of Canada

# Cyber security and risks related to electronic information management

Ransomware, phishing, and other cyber attacks use vulnerabilities in order to access sensitive research data, information, or knowledge that is not publicly available. Organizations can contact the Canadian Centre for Cyber Security for information about available cyber defence services, or take advantage of free tools and services like the Cyber Security Audit Program. They are also encouraged to undertake the Top 10 IT security actions.

**Mitigation measures include:**

- updating devices and applications regularly and developing a life-cycle management strategy to replace obsolete equipment that create security vulnerabilities
- using multi-factor authentication, a virtual private network, strong passwords and encrypting stored data and communications between devices
- classifying and marking data based on risk, assigning access rights to users based on a need-to-know and deactivating accounts when users change roles or leave the organization
- backing up data regularly to an offsite storage location that is inaccessible by the organization's networks or Internet connections

- properly destroying sensitive information (including external storage devices)
- implementing a security log monitoring solution to detect anomalies, and segmenting networks to control traffic flows and access, and to help isolate and stop the spread of malware
- embedding cyber security and data security standards into the organization's service agreements with vendors, including verifying how data will be secured and handled by vendors
- reviewing and addressing potential cyber security gaps on a regular basis; consulting the Cyber Center's National Cyber Threat Assessment site for up-to-date guidance on cyber threats and mitigation measures
- conducting a security review of information disseminated to the public (e.g. Internet postings)

# Risks related to intellectual property (IP) sharing

An organization's partners, both inside Canada and abroad, may not share its interests on ownership, publication, and use of intellectual property, whether it is formally protected (via patents, trademarks, etc.) or not. Acquisition of, or access to background, foreground and other forms of research knowledge, IP or property may be used by a partner to access additional IP beyond the scope of a formal agreement and without recognition or compensation.

The Canadian Intellectual Property Office (CIPO) helps small-and-medium sized businesses understand the value of their IP and develop an IP strategy through its Intellectual Property Advisors. It also provides online learning tools and resources as well as information about applying for IP rights, enforcement and commercialization, and relevant government programs through the IP Village.

**Mitigation measures include:**

- determining the dual-use character of an organisation's research, data and assets, and being aware of applicable laws and regulations. A starting point is to review:
    - Canada's Export Control List, which lists certain goods and technologies for which a government-issued export permit is required; administered by Global Affairs Canada
    - Schedule B of the *Nuclear Non-proliferation Import and Export Control Regulations*, which lists nuclear-related dual-use items the import and export of which is controlled by the government; administered by the Canadian Nuclear Safety Commission
    - the Guide to the Schedule to the Defence Production Act to identify controlled goods. This pertains to goods and their associated technologies that have military or national security significance and are domestically controlled
    - the Emerging Technology Trend Cards catalogue designed to communicate information about technologies that may impact defence, public safety and national security
- developing best practices for sharing knowledge (public disclosure approvals, disclosure impacts to IP protections, publishing delays due to IP considerations like patent approvals)
- discussing and agreeing on the ownership of research outcomes with research partners and what rights each party has to the IP produced by the project
- avoiding the premature disclosure of new inventions to prevent loss of research knowledge, including IP rights, trade secrets or proprietary information and commercially valuable IP

# Requirements for defence-related research and innovation

Given the dual-use nature of some quantum technologies, there is a large demand for defence-related quantum research and innovation among domestic and foreign governments. The Security requirements for contracting with the Government of Canada indicate how PSPC's Contract Security Program (CSP) can help eligible organizations participate in Government of Canada, foreign government and other international contracts, such as by bidding on North Atlantic Treaty Organization procurement initiatives. It provides Organizational security screening and Personnel security screening. The security requirements for each contract are outlined in the security requirements checklist at the beginning of each bidding process, which determine the level of screening required. On average, security screening takes between one and six months depending on the level of screening required. Organizations anticipating the development of outputs with military or dual-use applications are strongly encouraged to engage early with the relevant federal contracting department and the CSP regarding security requirements. For more information, please Contact the Contract Security Program.

Note that beginning in winter 2025, suppliers seeking to bid or work on select Government of Canada defence contracts must also become certified under the Canadian Program for Cyber Security Certification (CPCSC). More information is available on the Cyber security certification for defence suppliers in Canada site.

Those working with Department of National Defense programs where collaborative arrangements are not designed as contracts, such as the Canadian Safety and Security Program (CSSP) or the Innovation for Defence Excellence and Security (IDEaS) program, should consult the corresponding applicant guides for information on research security requirements.

In addition, individuals and organizations need to register in the Controlled Goods Program (CGP) to examine, possess, or transfer goods and associated components and technology that have a military or national security significance. These are considered **controlled goods**, a subset of Canada's Export Control List, and can include blueprints and technical specifications. The CGP also assists registrants in achieving and maintaining compliance. The Guideline for developing a security plan for safeguarding controlled goods helps registrants develop a security plan for work sites where controlled goods are examined, possessed or transferred. A directory is also available to find individuals and organizations registered in the Controlled Goods Program.

Finally, organizations bidding or working on projects that require access to **unclassified military technical data** in Canada or the United States must be certified by the Joint Certification Program (JCP).[5] The program is managed through the Canada/US Joint Certification Office, which is jointly staffed by the Department of National Defence and US Department of Defence. Unclassified military technical data is a type of information (including blueprints, drawings, plans, computer software or technical documentation) that is used to produce military or space equipment and related technology, and unauthorized access to which could pose a threat to national security. It can include data which is used by universities to conduct research, and universities are eligible to participate in the JCP. The certification refers to both facility and employees (with some exceptions), and the review process is five business days with validity for up to five years.

[5] Handling unclassified military technical data: Joint Certification Program

# Other Government of Canada programs

The Regional Resilience Assessment Program (RRAP) administered by PSC is a vulnerability and dependency assessment program for Canadian critical infrastructure facilities, including quantum R&D facilities. It involves Cyber and Infrastructure Resilience Assessments to help organizations measure and improve their physical security and resilience to all hazards in Canada. Hazards include accidental or intentional human-made events, and natural catastrophes. Participants receive reports with security and resilience scores, peer comparisons, resilience enhancement options and a virtual rendering that can be shared with first responders.

Given the sensitive nature of quantum technologies, quantum R&D facilities are encouraged to get in touch with PSC and discuss whether an assessment would be a good fit for their risk profile and how it could help them achieve a resilience posture aligned with industries such as data centers, critical manufacturing sites and other research laboratories. Assessments are voluntary, non-regulatory, free-of-charge and confidential. The Critical Infrastructure Assessment Exploration tool allows organizations to contact the RRAP for more information.

The Insider Risk Assessment Tool (IRAT), administered by PSC, is a voluntary, virtual tool for Canadian critical infrastructure stakeholders to self-assess their organization's security posture as it relates to insider risk. Those who complete the IRAT will receive a detailed report which, when used in conjunction with the recommendations of the Enhancing Canada's Critical Infrastructure Resilience to Insider Risk document, provides useful information and guidance to help increase their organization's insider risk resiliency.

PSC in collaboration with CSE and the Cyber Centre has also developed two Cyber Assessment Tools, namely the Canadian Cyber Security Tool (CCST) and the Canadian Cyber Security Tool 2.0 (CCST 2.0). These are virtual, voluntary self-assessment tools intended for Canadian critical infrastructure owners and operators. They provide participants with an overview of their organization's operational resilience and cyber security posture, as well as comparative results across their sector.

# Conclusion

Canada's quantum sector is growing, not least due to the open and internationally connected nature of our research ecosystem. In the context of intensifying global competition for quantum technologies, however, Canadian researchers and companies must increase their awareness of emerging threats to their work by state and non-state actors. They must also consider the security implications of research on technologies with dual-use potential. This document will be periodically updated to include new tools, resources and advice as the international security landscape evolves.