Public Safety Canada | Sécurité publique Canada

Canada

AT A GLANCE:

Research Security Information Update

February 2022

Notable Developments in Research Security

September 2021: Public Safety's Economic Security Task Force completed consultations on economic-based threats to national security that included research security as a key topic. The results of the consultations are being analyzed and will feed into the possible development of policy options for research security in the context of economic security.

July 12, 2021: The Minister of Public Safety and Emergency Preparedness, the Minister of Innovation, Science and Industry and the Minister of Health released Canada's National Security Guidelines for Research Partnerships. These guidelines integrate national security considerations into the evaluation and funding of research partnerships, and will assist researchers, research organizations, and the federal government in applying enhanced and risk-based due diligence assessments of research applications.

June 2021: The Government of Canada worked alongside its Group of Seven (G7) counterparts to advance Canada's research security priorities internationally. The inclusion of research security in both the G7 Leaders' Communiqué and the G7 Research Compact enhances the protection of research as a shared priority amongst Canada's closest allies and partners. Innovation, Science and Economic Development Canada will continue to advance these conversations in its role as Co-Chair of the G7 Working Group on the Security and Integrity of the Global Research Ecosystem.

May 2021: On May 20th, 2021, the Alberta government asked the province's four universities to pause any new partnerships with links to the Chinese government, review its existing relationships, and submit a report to the government. A few days later, Alberta called for national security rules for academics to prevent intellectual property transfer to China. This article provides insight to the steps the Government is taking to address this issue and points to efforts implemented by like-minded partners.

May 2021: The China Defence Universities Tracker has been updated. The tracker is a database of Chinese institutions engaged in military or security-related science and technology research created by the ASPI's (Australian Strategic Policy Institute) International Cyber Policy Centre.

April 2021: At the Virtual Five Country Ministerial, ministers from Canada, the United States, Australia, the United Kingdom and New Zealand agreed to cooperate on research security issues. The Communiqué states that the Five Eyes countries are "committed to work together, along with likeminded countries through multilateral fora, to share experiences and report on our progress to build collective resilience in the academic, research and development sectors against foreign interference and the unwanted transfer of knowledge."

Case Study Spotlight

Canadian institutions are at the forefront of innovation, research and development in several areas. The following scenario is inspired by a real life example that demonstrates why it is necessary to be proactive and take steps to mitigate threats from hostile actors.

A Canadian university was hosting an international scientific conference on a field that has dual-use applications. During one of the breaks between presentations, an unidentified individual went to the podium and inserted a USB thumb drive into the presentation laptop. The organizers and attendees noticed some file shuffling on the screen, but thought nothing more of it since the person could have been the next presenter uploading the latest version of their presentation.

This individual did not present in any of the sessions, and was later found taking pictures of poster presentations, which was against conference rules. The organizers approached the individual. He claimed that he had done nothing wrong, became confrontational while trying to evade questions, and attempted to leave the premises.

The individual was a foreign scholar visiting the Canadian university to pursue a short-term developmental opportunity, albeit in an unrelated field. Further investigation found that he had in fact illicitly copied a number of conference presentations to his USB key while on the podium. It was also determined that the foreign scholar was not even invited to attend the conference, nor had he registered or paid the registration fee. Fortunately, the flagrant breach of academic etiquette and potential theft of intellectual property was reported to the conference authorities. Without knowing what the foreign scholar's intentions were with the stolen information, it is possible Canada's security interests could have been harmed had he been successful.

What would you do in this situation?

It is important to:

- be mindful of dual-use applications of your research, and put in place effective measures to protect your research;
- understand that threat actors do not share the same values and ethics, or follow the same research policies as you;
- if safe to do so, challenge individuals who may be in places they should not be; raise questions to verify and clarify their purpose for being where they are (e.g. "Can I help you find something?"; "Are you here with someone?");
- put in place checks and protocols to establish the credibility of individuals who may be visiting your institution, labs or attending events, such as conferences, that you may be organizing;
- report any suspicious or criminal behaviour to the local police; and,
- in case of unanswered questions, report any concerns to relevant authorities (the Royal Canadian Mounted Police; Canadian Security Intelligence Service – see contact information below).

Physical Security Insight

In addition to ensuring one's institution has a good cyber security posture, it is important to pay attention to physical security measures. The Government of Canada defines physical security as the implementation of physical safeguard measures to prevent and delay non-authorized access to assets, information, people and services, to detect attempted or actual non-authorized access, and to trigger an appropriate intervention. Physical security safeguards can be applied to general building security, lab security, and office security.

Elements of Effective Security Measures for a Research Lab

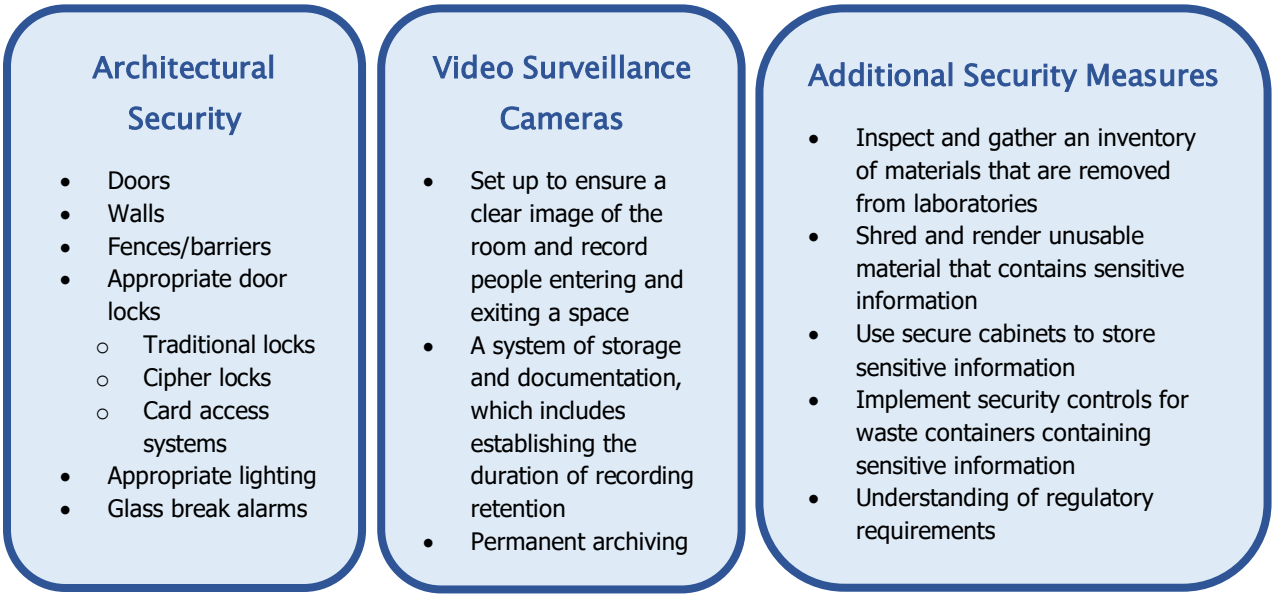

Figure 1: Elements of Effective Security Measures for a Research Lab

This figure depicts the elements of effective security measures for a research lab. These elements can serve as a checklist to ensure your information is protected against threat actors. The first element focuses on architectural security, the second element focuses on video surveillance cameras, and the third element provides additional security measures that can be implemented such as shredding documents containing sensitive material, inspecting and inventorying material, implementing security controls for waste containers, and securing cabinets.

Resources to Assess Physical Security

The Regional Resilience Assessment Program (RRAP) is a vulnerability and dependency assessment program for owners and operators for critical infrastructure facilities within Canada. This program involves site assessments to help organizations measure and improve their resilience to all hazards in Canada, such as cyber threats, accidental or intentional man-made events, and natural catastrophes. These site assessments are voluntary, non-regulatory, free-of-charge and confidential. The physical security component of the RRAP is comprised of two tools:

- Critical Infrastructure Resilience Tool (CIRT) (1 day to complete)
    - The CIRT is an on-site, survey-based tool that measures the resilience and protective measures of a facility. Outputs include a report and interactive dashboards that provide scores and peer comparisons, and highlight dependencies and resilience enhancement options for physical security, resilience, and cyber security.
- Critical Infrastructure Multimedia Tool (CIMT) (1/2 day to 1 day to complete)
    - The CIMT is a virtual rendering of a facility based on floor plans. It features panoramic photographs of interior and exterior significant areas and can be shared with first responders and/or used in exercises. Although doing so is at the discretion of the organization, we highly encourage sharing the CIMT with first responders so it can be used as a tool to prepare for, and respond to, emergency situations.

Critical infrastructure owners and operators can contact ps.rrap-perr.sp@ps-sp.gc.ca to discuss the possibility of having an assessment of their facility. Members are available to provide an interactive presentation to further explain the program and the products provided.

Want to know more?

Need help or have questions? Want to stay up to date and find out more on all things research security? Please send us an email at safeguardingscience-scienceensecurite@ps-sp.gc.ca or visit our Safeguarding Science webpage.

Public Safety Canada aims to continually publish useful information for the Canadian research community on relevant research security issues. We would like to hear from you! Are there specific products, tools, or information you would like to receive (i.e. on emerging risks/threats, research security case studies, statistics, guidance on key issues, security best practices, etc.)? Please send any suggestions you have to the Safeguarding Science email listed above.

Want to Report an Incident?

RCMP – National Security Information Network (NSIN)
Reporting of unrecognized persons, suspicious incidents, or computer-related activities.

Phone: 1-800-420-5805 Email: NSIN_RISN@rcmp-grc.gc.ca

Canadian Security Intelligence Service (CSIS)
Reporting of potential non-urgent national security threats or suspicious activities.

Phone: 1-800-267-7685 Website: Reporting National Security Information

Canadian Centre for Cyber Security (CCCS)
The CCCS Contact Centre is the single point of contact for questions on Cyber Security.

Phone : 1-833-CYBER-88 Email: contact@cyber.gc.ca

Please note that there is no planned publication schedule for the Research Security Information Update. Public Safety Canada will provide information as it arises or becomes available to our audience.

ISSN: 2564-1476
Cat. No.: PS7-2E-PDF