University of Regina

Newsline	Research Security		
Week	Sept. 29-Oct. 3, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Resource Package			
1	Team Canada – Mitacs Research Security		
2	Research Security Centre		

Executive summary: This report summarizes key developments in research security for the week of September 29, 2025, highlighting both domestic policy implementation and the global landscape of threats and opportunities. The insights are drawn from Mitacs's official Research Security Plan presentation and the Public Safety Canada / Research Security Centre's Weekly Newsline.

Mitacs solidifies its Research Security framework

A major domestic development is the continued implementation of Mitacs's updated Research Security Plan across its core programs. The Team-Canada update shows Mitacs has operationalized a rigorous due-diligence process aligned with federal National Security Guidelines for Research Partnerships and the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC).

Key operational takeaways:

- **Mandatory Declarations:** All applicants (academic supervisors, interns, industry partners) must declare any affiliations with Named Research Organizations (NROs) and whether their project advances a Sensitive Technology Research Area (STRA). A "Yes" to both can result in ineligibility.
- **Risk–Benefit Assessment:** Mitacs evaluates industry partners based on their presence in Canada, foreign government ownership, sanctions status, and potential identification by security agencies.
- **Proactive Measures:** Mitacs reserves the right to decline funding, impose conditions, or request additional information where risks are unacceptable or not clearly mitigated.

This framework represents a mature, operational approach to safeguarding Canadian research and IP, particularly in sensitive areas like AI, biotechnology, and cleantech.

Threats and pressures

The RSC Weekly Newsline highlights several international developments with direct implications for Canadian research security:

- **Cyber espionage intensifying:** European Network and Information Security Agency (ENISA) has warned of increased state-backed cyber espionage campaigns linked to China and Russia, targeting public institutions and research infrastructure. This underscores the need for heightened cyber hygiene within the research ecosystem.
- **Strategic competition for talent and technology:** China introduced a new "K visa" to attract global Science, Technology, Engineering, and Mathematics (STEM) graduates, while the U.S. has tightened its visa policies. At the same time, the European Research Council has reported a fivefold increase in applications from U.S.-based researchers, reflecting a broader shift in talent flows.
- **Political interference in academia:** Reports indicate U.S. policies are constraining academic freedom, prompting many researchers to consider relocation to Europe.
- **Academic boycotts:** Israeli universities are experiencing an unprecedented surge of boycotts linked to the military offensive in Gaza. Nearly 1,000 scientists have called on European Council for Nuclear Research (CERN) to rethink its collaboration with Israel. Academic invitations are being rescinded, projects put on hold, and about 30 European universities have terminated their partnerships.