University of Regina

Newsline	Research Security		
Week	Dec. 1-5, 2025		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		

Executive summary: This weekly Newsline finds research security rapidly shifting toward regulatory tightening, operational enforcement, and closer scrutiny of strategic investments. Provincial bills in Ontario and Quebec signal greater oversight of university research planning, a Stanford probe highlights vulnerabilities in foreign collaborations and disclosure compliance, and Canada's large investments in AI compute, fusion research, and Electric Vehicle (EV) materials raise high value IP risks. Procurement and supply chain concerns, illustrated by RCMP restrictions on hundreds of Chinese-made drones, persist. Overall, the landscape is moving to formal, mandatory, risk-based practices, and institutions must balance compliance, talent attraction, innovation, and sovereignty.

Key Points:

- **National policy shifts affecting institutional autonomy and research security:** Ontario's Bill 33 expands provincial authority over student fees and introduces mechanisms to regulate institutional research security plans. Quebec's Bill 1 may restrict universities' ability to challenge government decisions, raising concerns about autonomy.
  What this means: These developments indicate a trend toward stronger governmental intervention in university governance. For research security, mandatory, standardized frameworks may soon be required. Institutions should be prepared for external audits, compliance timelines, and greater alignment between university governance structures and provincial security expectations.
- **Stanford foreign collaboration case, oversight gaps and export-control risk:** A Stanford Review investigation alleges that a department chair maintained long-term, undisclosed collaborations with the High-Pressure Science and Technology Advanced Research Center (HPSTAR). The article links HPSTAR to elements of China's nuclear research programs and claims it appears on the U.S. Entity List. Reported activities include co-authored publications, hosting students, and use of federally funded research facilities.
  What this means: If accurate, this represents a serious case of disclosure failure and potential export-control exposure. It highlights vulnerabilities in conflict-of-interest reporting, monitoring of long-term partnerships, and researcher awareness regarding Entity List organizations. The case also demonstrates how reputational damage and compliance risk can arise quickly from unvetted collaborations.

- **Strategic investments in critical technologies, high-value IP, and infrastructure protection:** Recent funding announcements highlight growing national focus on sensitive and high impact research areas. These include $42.5M for AI compute infrastructure at the University of Toronto, a $92.5M federal–provincial investment in fusion energy research, ongoing work at the University of New Brunswick on magnetic materials critical to EV supply chains, and Quebec's $10M initiative to recruit researchers in strategic sectors. These fields generate sensitive data and commercially valuable IP that require stronger protection.

  What this means: Newly funded strategic initiatives will be high value targets for foreign intelligence and commercial espionage. Institutions must integrate security-by-design into project inception: access controls, contract clauses, cybersecurity standards, visitor management, and robust partner vetting. Early intervention prevents costly retrofits and mitigates IP leakage risk.
- **Procurement and supply-chain security, RCMP drone restrictions:** The RCMP restricted about 80% of its drone fleet (973 drones, mostly DJI) from sensitive operations due to security vulnerabilities, including risks related to data exposure and communications interception. Replacement costs could exceed $30 million.

  What this means: This is a direct example of supply chain exposure in operational settings. Universities increasingly rely on Chinese-origin hardware (drones, sensors, AI chips, laboratory instrumentation). Without origin-based risk screening, research data may be vulnerable to foreign access, telemetry collection, or firmware exploitation.
- **International research security frameworks, global trends and talent implications:** Switzerland is establishing centralized knowledge-security coordination and introducing risk-based screening for applicants from high-risk countries. In the United Kingdom (UK), newly tightened visa rules have drawn criticism for undermining university competitiveness and limiting access to international talent.

  What this means: Peer nations are formalizing national research security infrastructures. Canada is following suit, so universities must prepare for centralized reporting, standardized screening tiers, and coordinated training programs. The UK example shows the danger of over tightening: security measures must not undermine international talent recruitment.

Conclusion: Research security is becoming a central operational, regulatory, and strategic priority for universities. Legislation, foreign collaboration cases, and major investments in critical technologies highlight compliance gaps and emerging risks across talent, equipment, partnerships, and data. Institutions must adopt integrated, risk-based frameworks that combine due diligence, policy updates, supply chain security, training, and clear communication. Treating research security as an enabler of responsible scholarship allows universities to protect people and IP, comply with regulations, and remain globally competitive.