Newsline	Research Security		
Week	Jan. 26 - 30, 2026		
Editor	Alaa Dabboor	**Position**	Research Security Manager
Reference Package			
1	Research Security Centre		
2	Microsoft and Data Law blog, Microsoft legal compliance and transparency guidance		

Executive summary: This week highlights the critical need to protect sensitive research while supporting innovation in Canada. Internationally, allied efforts toward digital and research sovereignty, including reducing reliance on U.S.-based platforms like Microsoft Teams and Zoom, underscore strategic risks. Domestically, Quebec's Venture Scientist fund and Manitoba's biosecure labs aim to retain talent, while federal agricultural cuts and weak open-access enforcement reveal vulnerabilities. Recent developments, including an AI trade-secret theft conviction and the appointment of Canada's first foreign influence transparency commissioner, emphasize that research security is essential for economic competitiveness and national resilience.

Key Points:

- **Allied approaches to research and digital sovereignty:** France's initiative to develop a sovereign videoconferencing platform reflects concerns that reliance on U.S.-based services, such as Microsoft Teams and Zoom, could create cross-border data access risks. **Context**: U.S. law (the CLOUD Act, 2018) can, in certain circumstances, compel U.S.-based providers to produce data in their possession, even if that data is stored outside the United States.
- **What this means:** These developments underscore the importance of proactive data-governance strategies for Canadian institutions. Even when data is stored domestically, cross-border legal obligations can create potential exposure. Institutions such as the University of Regina should implement early strategies to mitigate data-sovereignty risks, because hosting data in Microsoft data centres physically located in Canada may not fully prevent disclosure to U.S. authorities in certain legal scenarios. Technical, contractual, and policy safeguards are essential to maintain control over sensitive data, ensure compliance with Canadian privacy and security requirements, and preserve research and institutional sovereignty in an increasingly globalized and legally complex digital environment.
- **Quebec's AI commercialization initiative:** Quebec launched a $100 million Venture Scientist fund to support AI researchers in commercializing discoveries while remaining active in research, with the goal of retaining talent and intellectual property in Canada.
  What this means: Domestic commercialization pathways reduce the risk of foundational AI research and talent migrating abroad or being acquired by state-linked foreign entities. Proactive retention strategies strengthen national research sovereignty.

- **Open-access policy gaps in federally funded research:** Canada's Tri-Agency open-access policy lacks effective enforcement, leaving many publicly funded research outputs behind paywalls or inconsistently accessible.

  What this means: Limited access makes it harder for government departments to identify and assess emerging risks, including dual-use applications and foreign influence. Stronger compliance would improve transparency and support research security assessments while protecting legitimate intellectual property.
- **Agricultural research capacity reductions:** Agriculture and Agri-Food Canada announced closures of multiple research facilities and significant staff reductions, raising concerns about long-term impacts on agricultural science.

  What this means: Reduced domestic research capacity weakens Canada's ability to address food security, biosecurity threats, and supply-chain resilience, increasing reliance on external expertise and partners.
- **Manitoba's investment in biosecure research infrastructure:** Manitoba committed $16.8 million to expand vaccine development, biomanufacturing, and high-containment laboratory capacity through new research centres.

  What this means: Strengthening domestic high-security lab infrastructure supports oversight of sensitive research, reduces dependence on foreign facilities, and helps retain specialized expertise in Canada.
- **AI trade-secret theft conviction:** A United States federal jury convicted a former Google engineer for stealing thousands of confidential AI documents intended to benefit a China-based startup.

  What this means: The case highlights the persistent insider threat to foundational technologies and underscores the need for robust data governance, access controls, and cross-sector awareness in both industry and academia.
- **Foreign influence transparency governance:** The federal government has proposed appointing Canada's first foreign influence transparency commissioner as part of new legislative oversight measures.

  What this means: Dedicated governance and transparency mechanisms enhance the ability to identify and manage covert foreign influence risks in research environments.

Conclusion: This week's developments highlight that research security is critical to innovation, economic competitiveness, and national resilience. Effective approaches combine investment in domestic talent and infrastructure with policy enforcement, insider-threat mitigation, and collaboration oversight. International trends, including digital-sovereignty initiatives and recent espionage cases, show research is increasingly a domain of strategic competition. Coordinated action is needed to protect Canada's research ecosystem while supporting collaboration with trusted global partners.