University of Regina

Newsline	Research Security	**Week**	May 4 – 8, 2026
Editor	Alaa Dabboor	Research Security Manager	
Reference Package			
1	Research Security Centre		
2	U.S. Department of the Treasury – Office of Foreign Assets Control (OFAC)		
3	Financial Action Task Force (FATF)		
4	U.S. Department of Commerce – Bureau of Industry and Security (BIS)		

Executive summary: This week highlights a research security environment shaped by cybersecurity risk, AI adoption, strategic infrastructure, and geopolitical pressure. A major cyberattack underscores reliance on digital systems, while AI integration introduces new governance challenges. At the same time, investments in semiconductors, telecommunications, and Arctic research signal a shift toward trusted, domestic capability. Global collaboration is becoming more constrained amid policy uncertainty, increased scrutiny of researchers and affiliations, and competition for talent and technology. Foreign interference, supply chain risks, and agentic AI further reinforce the need for coordinated, early-stage risk management, with research security increasingly defined by the intersection of infrastructure, partnerships, data, and strategic competition.

Key Points:

1. **Cybersecurity risks are impacting core academic systems:** A cyberattack on the Canvas platform disrupted access across thousands of institutions, including Canadian universities, highlighting reliance on shared systems and potential exposure of sensitive data.

   What this means: Cybersecurity is directly tied to academic continuity and research operations, requiring stronger coordination across IT, privacy, and research security.
2. **AI is being integrated into research development:** The University of Alberta is deploying AI tools to support grant writing and research development, with privacy safeguards to keep data within institutional environments.

   What this means: AI can scale research support but requires clear guidance on approved tools, data handling, and appropriate use.
3. **Strategic infrastructure and trusted networks are expanding:** Canada is strengthening domestic capacity in photonic semiconductors and AI while expanding telecommunications security cooperation, including EU participation in a global coalition.

   A proposed Arctic research centre linked to submarine procurement highlights growing investment in dual-use technologies with civilian and defence applications.

   What this means: Research infrastructure is increasingly viewed through a security and competitiveness lens, with emphasis on trusted domestic capacity and allied partnerships.
4. **Foreign interference, espionage, and talent transfer risks persist:** CSIS identifies multiple states engaged in espionage, cyber operations, and influence activities.

   Cases involving talent movement to China and espionage activity in the UK reinforce risks related to affiliations, access to data, and transnational repression.

   Sanctions and enforcement approaches are also shifting toward network-based targeting, including individuals, front companies, and joint ventures, increasing the complexity of due diligence.

What this means: Institutions should continue strengthening due diligence on partnerships, affiliations, and access to sensitive research.

5. **International collaboration is becoming more constrained and scrutinized:** Global collaboration continues to expand (e.g., UBC joining the Eurolife Network), but new pressures are emerging.
   Policy uncertainty around National Institutions of Health (NIH) funding, increased oversight of foreign contacts (South Korea), and evolving governance structures in global research systems are reshaping engagement.
   Canada ranks highly globally but faces gaps in funding and translating research into application.
   What this means: Institutions must balance openness with compliance, disclosure, and geopolitical risk considerations.
6. **Supply chain and dual-use risks remain difficult to control:** Chinese firms continue supplying drone components through complex global networks despite sanctions, while countries such as Australia and Japan strengthen cooperation on AI, critical technologies, and resilient supply chains.
   These risks are reinforced by ongoing challenges in enforcing sanctions and export controls, particularly in advanced and dual-use technologies.
   What this means: Dual-use risks extend beyond restricted items, requiring stronger supply chain awareness and due diligence.
7. **Agentic AI introduces new and evolving security risks:** Five Eyes cybersecurity agencies warn against granting autonomous AI systems broad access to sensitive data or critical systems due to risks of unintended actions and data exposure.
   What this means: AI governance should be integrated into institutional risk frameworks, with strict controls, limited deployment in higher-risk contexts, and human oversight.

Conclusion: Research security is increasingly a cross-cutting institutional function. Cybersecurity, AI, infrastructure, supply chains, and partnerships are becoming tightly interconnected. Universities will need earlier risk identification, clearer guidance for researchers, and stronger coordination across research, compliance, and IT functions to remain competitive and secure.

At the same time, increasing enforcement expectations and financial complexity are placing greater pressure on institutions to demonstrate documented due diligence and compliance with readiness.