HERSA The Higher Education Research Security Association

Monthly Membership Update

October 2026



Welcome to the latest edition of the HERSA monthly newsletter, bringing you key updates and insights to keep you abreast of national and international developments in research and economic security.

This Month's Highlights

- Invitation: UK-Canada Joint Statement of Intent Launch Webinar – 19 Nov
- RAEng New Paper – Understanding Dual-Use: Exploring the Tensions and Trade-offs
- NTE 2026/24: Proposed Amendments to UK Strategic Export Controls
- NCSC – Joint Cybersecurity Advisory: Integrity Technology Group
- ISDP's Research and Innovation Series (RIS) - New Research Security Webinar
- Defence Research and Development Canada (DRDC) Launches Research Security Policy
- European Commission Launches New Dual-Use Technologies Resource Hub
- Right-Sizing Research Security: New Insights from Australia
- New Vacancies

Invitation: UK-Canada Joint Statement of Intent Launch Webinar – 19 Nov

To our UK HERSA members, keep your eyes peeled for an invitation landing in your inbox next week for a **joint HERSA webinar with our colleagues from the Canadian Research Security Community of Practice ("Team Canada")**!

The webinar will take place at 3.30pm GMT on 19 November and **will mark the launch of the new UK-Canada Joint Statement of Intent**, which sets out a shared commitment to strengthening collaboration between our two research security communities. Delegates will hear more about the Statement, planned activities for 2027 and opportunities to become involved in future UK-Canada engagement.

Full details including joining information will be shared with members next week but for now, please save the date in your diary!

Please note, on this occasion, the session will be limited to UK HERSA members.

© 2026 HERSA - The Higher Education Research Security Association

RAEng New Paper – Understanding Dual-Use: Exploring the Tensions and Trade-offs

The **Royal Academy of Engineering** has published a new paper, **Understanding Dual-Use: Concepts, Tensions and Trade-offs**, exploring how the term 'dual-use' is applied across research, innovation, economic and security contexts. Rather than seeking to establish a single definition or prescribe a particular approach, **the paper highlights the competing priorities and trade-offs that policymakers, researchers and institutions must navigate when assessing emerging technologies.**

Drawing on extensive stakeholder engagement, it examines how different interpretations of dual-use can lead to inconsistent or unintended outcomes and encourages greater consideration of the wider system impacts of policy decisions. The paper provides a timely contribution to ongoing discussions around responsible innovation, research security and technology governance.

Notice To Exporters 2026/24: Proposed Amendments to UK Strategic Export Controls

The **Export Control Joint Unit (ECJU)** has published **advance notice of proposed amendments** to the UK's Strategic Export Control framework, with **regulations expected to come into force in early December 2026**.

The proposed changes would update controls on military and dual-use goods, software and technology, reflecting outcomes from the 2025 multilateral export control regime reviews and **introducing revised controls on certain advanced and emerging technologies, including semiconductor manufacturing equipment, advanced computing technologies and specialised materials.**

The notice also outlines updates to Schedule 4 country listings and the planned revocation of General Export Authorisation No. 001 (GEA001), which has been superseded in Great Britain by the Dual-Use Open General Export Licence.

NCSC – Joint Cybersecurity Advisory: China-linked Malicious Actors Called Out for Targeting Sensitive Data

Earlier this month, the **National Cyber Security Centre (NCSC)**, alongside international partners (including Australia, Canada, Japan, New Zealand, Spain and the United States), attributed malicious cyber activity targeting sensitive data globally to actors linked to a China-based company, **Integrity Technology Group**.

The advisory **highlights how threat actors are increasingly combining AI-enabled tools, such as automated vulnerability scanning, with large-scale botnets and traditional exploitation techniques to identify and compromise targets.** The activity has affected organisations across multiple sectors, including critical infrastructure, and serves as a reminder of the evolving cyber threat landscape facing research, government and industry organisations. Institutions may wish to review the advisory and consider the implications for cyber resilience, data protection and risk management practices.

© 2026 HERSA - The Higher Education Research Security Association

Building Research Security Communities and Capability in Portugal

On 22 October, Chaitali Desai supported the delivery of the first European microcredential course in Research Security and Innovation at the **Universidade de Minho (Braga, Portugal)**, presenting sessions and workshops on two topics: The creation of a research security office from the ground up and building research security communities of practice, and the consideration of research security and due diligence in supply chain and procurement activities.

Drawing on her experience of establishing the Research Compliance function at the University of Bristol and **discussing HERSA's central role in fostering communities of practice**, this was a great opportunity to share expertise and support professional development for Portuguese colleagues. With support from British and U.S. Embassies and contributions from speakers representing universities across the U.S. and Europe, the sessions explored **proportionate due diligence, governance, practical risk management and the challenges of developing capability with limited resources.** HERSA's role in creating a UK-wide free resource to support universities and research institutions was highlighted, as attendees exchanged experiences, strengthened international connections and demonstrated the benefits of collaborative, practitioner-led approaches to research security.



ISDP's Research and Innovation Series (RIS) - New Research Security Webinar Available

The **Institute for Security and Development Policy (ISDP)** has released the latest webinar in its Research and Innovation Series (RIS), **Reframing Research Security for the Future of International Science and Technology Collaboration**.

In the session, David Biggs, Senior Fellow at ISDP, presents a **forward-looking perspective on how research security can evolve beyond a compliance and risk management exercise to support resilient, trusted and internationally connected research ecosystems**. The discussion examines how governments, universities, funders and researchers can respond to an increasingly complex security environment while maintaining the openness and international collaboration that underpin scientific progress.

Defence Research and Development Canada (DRDC) Launches Research Security Policy

Defence Research and Development Canada (DRDC) has launched a new **Research Security Policy** aimed at strengthening the protection of research projects, researchers, partnerships and intellectual property. The policy establishes a framework for embedding research security considerations throughout the research lifecycle and reflects Canada's continued focus on safeguarding sensitive research and innovation activities. While developed for DRDC-funded and DRDC-led research, the policy provides insight into the evolving research security landscape in Canada and may be of interest to institutions monitoring international approaches to managing research security risks, trusted collaboration and the protection of research assets.

© 2026 HERSA - The Higher Education Research Security Association

European Commission Launches New Dual-Use Technologies Resource Hub

The **European Commission** has launched a **dedicated webpage on Dual-Use Technologies**, bringing together information on **Commission initiatives**, **expert analysis** and reports, **upcoming funding opportunities** across 2026 and 2027, and other related resources.

The new resource provides a central point of access for stakeholders interested in the intersection of civilian and defence applications of technology, reflecting the growing prominence of dual-use considerations within European research and innovation policy.

Follow us on LinkedIn!

To help grow our page and the wider HERSA network, **follow us** and keep up to date with the latest news and events.

Right-Sizing Research Security: New Insights from Australia

The University of Technology Sydney's **Australia-China Relations Institute (ACRI)** has published two new reports examining how Australia's evolving research security landscape is experienced by Chinese-background scientists working in Australian universities. Drawing on both survey and interview findings, the reports explore perceptions of current research security policies, their impact on international collaboration, and researchers' sense of belonging within the academic community.

- Right-Sizing Research Security: A Survey of Chinese-Background Scientists in Australian Universities
- Right-Sizing Research Security in Practice: Interviews with Chinese-Background Scientists in Australian Universities

While respondents broadly supported the need for national security safeguards, many expressed concerns about the clarity and practical application of existing guidance, as well as whether current approaches appropriately distinguish between higher-risk and lower-risk research collaborations. The findings offer a timely contribution to ongoing discussions about balancing research security, international collaboration and research culture.

New Vacancies

Senior Research Security Advisor (3 posts)
Imperial College London
Closing date: 8th November 2026
London, UK
APPLY NOW

Export Control Compliance Lead
CERN, European Organization for Nuclear Research
Closing date: 20th November 2026
Geneva, Switzerland
APPLY NOW

Have a vacancy you'd like us to feature? **Get in touch!**

Disclaimer:
This newsletter is compiled using publicly available information from news outlets, social media and government websites. While we strive to ensure accuracy and use reputable sources, we do not endorse any specific media and we are not responsible for the reliability of external information. Links to original sources are provided, but their content does not necessarily reflect the views of HERSA or any member institution. We are not liable for any errors, omissions, or actions taken based on this information. Readers should verify details independently.

© 2026 HERSA - The Higher Education Research Security Association