

October 2025

Monthly Membership Update



Welcome to the latest edition of the HEECA 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

MI5 Director General Highlights Growing Security Risks for Universities

HEECA Secretariat Sets Course for the Future

OFSI Consolidated List to Close in January 2026

UK-U.S. Memorandum Highlights Research Security Cooperation

Strengthening Ties: HEECA at the EU Research Security Conference

EC Announces New Measures to Strengthen Research Security

Science Europe: Balancing Openness and Security in Research – New Report

Safeguarding Western Start-ups in Global Pitch Competitions

CCA Publish New Report: Balancing Research Security and Open Science

UK & RoI



MI5 Director General Highlights Growing Security Risks for Universities

MI5 Director General Ken McCallum recently delivered the agency's annual threat update, drawing attention to a sharp escalation in state-sponsored activity targeting UK institutions, including universities.

Key considerations for the sector include:

- A rise in espionage efforts focused on critical infrastructure and the theft of intellectual property
- Warnings about covert attempts to recruit UK-based academics through seemingly legitimate job offers
- A reminder for institutions conducting AI research to assess the security risks of their work and remain alert to potential state-sponsored threats.

As the UK faces a more complex and overlapping threat landscape, the sector is being called upon to play a vital role in safeguarding national interests.



HEECA Secretariat Sets Course for the Future

Last week, our secretariat gathered in the North West, generously hosted by colleagues at The University of Manchester, for a long-anticipated strategy workshop. The day offered a valuable opportunity to reflect on HEECA's achievements to date and to shape its future direction. Discussions were forward-looking and energised, laying the groundwork for several key developments, including:

- The transformation of HEECA's website into a **National Trusted Research, Education and Innovation Security Hub**
- Ongoing development of a **Trusted Research eLearning package** with the National Protective Security Authority (NPSA)
- Planning for a full and ambitious **2026 events calendar**
- Exploration of a range of collaborative opportunities

Crucially, we reaffirmed our commitment to advocating for the sector and championing research security across the UK.

We are especially grateful to our members for their thoughtful contributions, which have been instrumental in guiding our priorities. With momentum building, we look forward to sharing more as we move ahead with purpose.



OFSI Consolidated List to Close in January 2026

The **Office of Financial Sanctions Implementation (OFSI)** has confirmed that the Consolidated List of Asset Freeze Targets will close on 28 January 2026. From this date, the UK Sanctions List will become the sole authoritative source for all UK sanctions designations.

While the structure of the UK Sanctions List will remain unchanged, organisations currently using the OFSI list will need to update their systems and processes accordingly. Guidance has been published to support the transition, with the move aiming to simplify compliance and improve clarity across the sanctions regime.



UK-U.S. Memorandum highlights research security cooperation

The UK and United States have signed a Memorandum of Understanding to enhance collaboration in science, technology, and innovation. Among several areas of cooperation, the agreement notes the importance of research security in safeguarding critical and emerging technology research and development.

Both governments recognise each other's established approaches and commit to deepening collaboration to protect their technologies and people. This includes sharing effective practices and information on systems to identify and mitigate threats to the research enterprise, supporting capacity building across universities, research organisations, and industry, and strengthening cooperation on threat analysis in key technology areas. The two countries also aim to encourage allies and partners to adopt similarly rigorous standards, supporting a trusted international research environment.



International



EC Announces New Measures to Strengthen Research Security

Framing the opening day of this week's EU Research Security Conference, the European Commission has announced a series of **new measures to embed research security across the EU**, marking a significant shift in how research and innovation are safeguarded. For the first time, research security is set to be inserted in law through the forthcoming **European Research Area (ERA) Act**. The Commission emphasised that protecting research security is essential to preserving academic freedom, maintaining trust in open research systems and enabling Member States to respond effectively to emerging risks.

New initiatives include the creation of a **European Centre of Expertise on Research Security**, a **due diligence platform** to support international collaboration and a **common methodology for testing the resilience** of research-performing organisations (RPOs). These developments build on the Council's 2024 Recommendation on Enhancing Research Security and reflect a growing commitment to coordinated, proportionate and open approaches across the EU.



Strengthening Ties: HEECA at the EU Research Security Conference

Earlier this week, we attended the **European Commission's flagship Research Security Conference** in Brussels, joining partners from across the continent to explore shared challenges and opportunities. Clear themes emerged throughout the event, including the importance of openness, proportionality and unity in shaping effective research security frameworks.

It was encouraging to see strong UK representation across the agenda, offering valuable context and perspectives to our European counterparts. **HEECA's Jonathan Scott (University of Strathclyde) contributed to a key panel discussion with CESAER members**, sharing insights on how universities can begin implementing research security measures and offering an institutional perspective on strategy development and lessons learned.

Our thanks to the European Commission and organising partners for hosting a thoughtful and timely event that marks an important step forward in strengthening international collaboration on research security.



Follow us on LinkedIn!

We are on [LinkedIn](#). To help grow our page and the wider HEECA network, follow us and keep up to date with the latest news and events!



Science Europe: Balancing Openness and Security in Research – New Report

Science Europe has published its latest report on research security, drawing on a series of workshops held between January and June 2025. The report explores how research performing and funding organisations across Europe are responding to growing geopolitical pressures and the need to safeguard research without compromising openness, academic freedom, or international collaboration.

Key messages include the importance of proportionate risk management, the need for shared definitions and ‘red lines’ and the value of embedding research security through awareness-raising and cultural change. The report reinforces that research security should be seen not as a constraint, but as a framework that enables responsible, open, and resilient international collaboration. Full report linked.



Safeguarding Western Start-ups in Global Pitch Competitions

Latest in the **U.S. Safeguarding Our Future** series, the recently released **Safeguarding Western Start-ups** advisory, issued jointly with the **Canadian Security Intelligence Service (CSIS)**, warns that international pitch competitions, particularly those linked to the Chinese government or CCP, are being used to acquire Western technology and talent. While marketed as opportunities for investment and exposure, these events often require start-ups to disclose sensitive intellectual property, business strategies and personal data. The advisory highlights key mitigation steps, including conducting thorough due diligence on organisers, securing intellectual property before disclosure, limiting the information shared during pitches and engaging with national security bodies to report concerns and access guidance.

While not specifically directed at academia in this release, colleagues involved in spin-out or tech transfer activity should remain alert to these risks.



CCA Publish New Report: Balancing Research Security and Open Science

The **Council of Canadian Academies (CCA)** has recently published **Balancing Research Security and Open Science**, a report examining how Canada can protect sensitive research while maintaining its commitment to openness. Commissioned by **Defence Research and Development Canada** and the **Public Health Agency of Canada**, the report defines ‘sensitive research of concern’ as work that could be misused to threaten public health, national security, or economic interests.

The report emphasises that research security and open science are not mutually exclusive, advocating for a balanced, risk-informed approach. It outlines practical safeguards, including due diligence, cybersecurity, and pre-publication review and highlights the need for institutional support and training. Check-out the full report.



NEW VACANCIES

No vacancies this month, but check back next time.

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 HEECA or any member institution. We are not liable for any errors, omissions, or actions taken based on this information. Readers should verify details independently.