

September 2026

Monthly Membership Update



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

National Security (State Threats) Act 2026

New HERSA Insight: Engagement with the National Security and Investment Act

Join Us at This Year's EC&S Symposium

UUK: Research, Skills, Collaboration – How Universities Power UK Security

Science Diplomacy: Sovereignty, Strategy, and the Global Race: Government Response

UKRI Research on Research Security Hub

How the UK Should Protect its Science and Tech Research from Foreign State Threats

Ireland Publishes First National Research Security Guidelines

EU Updates Dual-Use Control List

Early Lessons from Finland's Research Security Requirements

ENCORS 2027 Call for Session Proposals Now Open

New Guidance for Canadian Businesses Travelling Abroad

National Security (State Threats) Act 2026

The National Security (State Threats) Act 2026 received Royal Assent on 8 July 2026, introducing significant new powers to counter hostile state activity. The legislation enables the Home Secretary to designate organisations involved in state threat activity, creating a regime broadly equivalent to proscription under terrorism legislation.

The new framework is designed to strengthen the UK's ability to disrupt and deter state-linked organisations, including proxy bodies operating on behalf of foreign actors. New criminal offences will apply to individuals who support, assist or derive material benefit from designated organisations. Those acting for or on behalf of a designated body may face prosecution under national security legislation, with penalties of up to 14 years' imprisonment for the most serious offences.



New HERSA Insight: Engagement with the NSI Act

The HERSA NSI Subgroup has published a **summary report of the National Security and Investment (NSI) Act survey** conducted with members ahead of the Annual Conference earlier this year. The report brings together key findings, recommendations and practical experiences from across the membership, **providing valuable insight into how institutions are engaging with the NSI regime**.

The findings have now been published, providing valuable insight into current sector practice and levels of engagement with the NSI process, as well as areas where further guidance and knowledge-sharing may be beneficial. **We encourage members to review the report and continue contributing to future initiatives** as the community develops its understanding of NSI-related challenges and good practice.



Join Us at This Year's EC&S Symposium

HERSA will be attending the DBIST **Export Control and Sanctions (EC&S) Directorate Annual Symposium** on 14 October, where we will be exhibiting within the Knowledge Hub and delivering a workshop session on 'Working with Academia: collaboration, compliance and research security'.

The symposium will provide attendees with the latest updates on UK export controls and sanctions, with contributions from EC&S operational and policy teams. **Registration has now reached capacity, but a waitlist remains available for prospective attendees.** If you are attending, we would be delighted to see you so please visit us in the Knowledge Hub, or join our workshop session!



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.



UUK: Research, Skills, Collaboration – How Universities Power UK Security

A new report from Universities UK explores how UK universities are strengthening national security **through research, skills development, innovation and collaboration with government and industry**. The publication highlights the growing contribution of higher education to defence capability, from advanced research programmes through to developing the specialist workforce required for future security challenges.

The report also includes the **newly announced founding membership of the Defence Universities Alliance (DUA)**, a partnership between universities, the Ministry of Defence and the wider defence and national security community. The Alliance comprises 35 universities selected from almost 100 applicants and has been established to advance defence-related research, build critical skills pipelines, and strengthen collaboration across academia, government and industry.

The publication offers useful insight into the evolving role of universities in supporting the UK's long-term defence, security and resilience ambitions.



Science Diplomacy: Sovereignty, Strategy, and the Global Race: Government Response

The Government has published its response to the House of Commons Science, Innovation and Technology Committee's report on science diplomacy, **broadly accepting the importance of aligning international scientific collaboration with the UK's economic, security and foreign policy objectives**. The response highlights ongoing investment in research, innovation and talent, while emphasising the need to balance ambition with fiscal constraints, national security considerations and commercial sensitivities.

Key themes include **strengthening international science partnerships, developing sovereign capability in critical technologies, attracting and retaining global research talent and supporting innovation through investment and procurement**. The Government also reiterated its commitment to a more strategic approach to technology resilience through the 'own-collaborate-access' framework and **confirmed that a UK Research Security Strategy will be published later this year**, alongside a dedicated fund to support research institutions in managing security risks.

For universities and research organisations, the response provides further insight into how the Government intends to balance openness and international collaboration with increasing focus on resilience, economic growth and national security priorities.



UKRI Research on Research Security Hub

UKRI has announced plans to establish a new Research on Research Security Hub, which will **serve as a national focal point for research security evidence, capability building, community development and innovation**. Led by EPSRC, the Hub aims to strengthen the evidence base underpinning effective research security practices across the UK research sector.

The initiative will receive **£6.25 million in funding through a single award** and is expected to launch in October 2026. The Hub is intended to support the development of research security expertise and help organisations navigate an increasingly complex security landscape.



How the UK Should Protect its Science and Tech Research From Foreign State Threats

A new research paper released by Chatham House explores how the UK can better protect science and technology research from foreign state threats while maintaining the international collaboration that underpins research excellence.

The paper argues that, **although the UK has strengthened its research security framework in recent years, current measures remain fragmented and largely reactive**. It calls for a more strategic approach, including stronger coordination across government, research funders and universities, greater transparency around international partnerships, enhanced institutional capability and improved risk management throughout the research lifecycle.

Central to the paper is the challenge of safeguarding the UK's research assets, knowledge and intellectual property without isolating the sector from the global partnerships that drive innovation and scientific advancement.



Ireland Publishes First National Research Security Guidelines

The Department of Further and Higher Education, Research, Innovation and Science has published **Ireland's first national research security guidelines**, establishing a coordinated approach to managing security risks associated with international research and innovation collaboration.

The guidelines are **intended to support open and productive international partnerships** while helping research organisations identify, assess and manage emerging risks in a proportionate and context-sensitive manner. The framework includes measures aimed at **protecting against intellectual property theft, foreign interference, cyber threats and the misuse of sensitive research**, aligning Ireland's approach with international research security best practice.



EU Updates Dual-Use Control List

The European Commission has updated the **EU Dual-Use Control List (Annex I of Regulation (EU) 2021/821)**, bringing it into line with changes agreed through key international export control regimes during 2025. The update is **intended to strengthen controls on emerging and strategically important technologies**, while maintaining a consistent approach across EU Member States.

Newly controlled items include certain **semiconductor manufacturing and testing equipment, advanced computing integrated circuits, additive manufacturing equipment for energetic materials, silicon carbide production technologies, ceramic matrix composites for high-temperature applications and technologies relating to gas turbine engines**. The changes form part of the EU's wider efforts to ensure export controls keep pace with technological developments and evolving security considerations.



Early Lessons from Finland's Research Security Requirements

The **Research Council of Finland** has published reflections from the first funding call to include **mandatory research security requirements**. The review found that the new process has been implemented successfully, with research security increasingly recognised as an integral part of responsible research planning and delivery.

Importantly, **the introduction of research security assessments appears to have had only a limited impact on international collaboration, reinforcing the message that research security is intended to enable secure collaboration rather than restrict it**. Feedback from applicants has been broadly positive, with many researchers drawing on support from institutional research services when preparing risk management plans. Updated guidance and application materials have since been published to reflect lessons learned from the first application round.



ENCORS 2027 Call for Session Proposals Now Open

The organisers of the **ENCORS Conference 2027** taking place at TU Delft on 25-26 May, have **launched a call for session proposals** and are inviting the research security community to help shape the programme.

The team have emphasised a preference for participative formats that encourage discussion and knowledge exchange over traditional panel sessions. **Have an idea, experience or best practice worth sharing?** Submit a proposal and help shape the conversation at ENCORS 2027! The deadline for submissions is 15 October.



New Guidance for Canadian Businesses Travelling Abroad

The **Government of Canada** has published new **guidance on research security for businesses travelling abroad**, aimed at helping organisations protect research, innovation and intellectual property from interference, theft and other security risks.

Built around four key themes, understand the **threats, assess your risk profile, know your research and know your partner**, the guidance encourages organisations to consider issues such as sensitive technologies, export controls, critical infrastructure, foreign influence and sanctions when engaging in international collaborations.

The guidance emphasises that research security is intended to support, not restrict, international collaboration by helping organisations make informed and proportionate risk-based decisions.



U.S. DoW Orders Research Security Audits at 30 Academic Institutions

In July, we highlighted developments relating to **Section 1286 of the U.S. FY19 NDAA**, which restricts U.S. Department of War (DoW) funding where institutions maintain certain relationships with designated foreign entities. Last month, **the DoW announced a significant escalation in its oversight activity**, directing 30 academic institutions to undertake immediate and comprehensive reviews of their research, financial and academic collaborations with foreign entities of concern.

The reviews **examine active partnerships with organisations identified under Section 1286**, as well as entities linked to rebranded Confucius Institutes. To maintain eligibility for future federal research funding, affected institutions must assess exposure to sensitive and export-controlled research, identify potential vulnerabilities and implement mitigation measures, including the termination of higher-risk partnerships where necessary.

The announcement reflects the continued emphasis being placed on research security, technology protection and foreign influence risks within the US research and higher education sector and may provide a further indication of the direction of travel for research security policy in the US.



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.