

Monthly Membership Update

February 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

HERSA Rebrand Now Live!

Defence Research Security: MOD, Dstl and HERSA Subgroup Collaboration

HERSA and KE UK Webinar – 24 March, 12pm

New DfE Guidance: Protecting UK Higher Education from Foreign Interference

MOD Announce £80m Student Skills Investment to Boost UK Defence

UK Vice Chancellors Receive Security Briefing

Export Control Joint Unit: 2026 Upcoming Webinar Opportunities

HERSA at ASCE 2026: Securing Knowledge Across Borders

New Vacancies

HERSA Rebrand Now Live!

Thank you to everyone who joined our virtual rebrand launch session earlier this week. It was great to see such strong interest and support as we move forward from HEECA.

If you were unable to attend, we will shortly share a summary of the key updates along with an anonymised version of the Q&A.

Our domain and contact details have now changed:

www.heeca.org.uk → www.hersa.co.uk
enquiries@heeca.org.uk → enquiries@hersa.co.uk

We have an active year ahead, so keep an eye out for further announcements!

Think you're not receiving our emails?

Get in touch and we can provide you with a template to share directly with your IT team to ensure HERSA doesn't get lost in mail filtering / security systems.

Defence Research Security: MOD, Dstl and HERSA Subgroup Collaboration

The Defence Science and Technology Laboratory (DSTL) and the Ministry of Defence (MoD) have published new guidance to support universities and researchers working with UK Defence. **Developed collaboratively with the HERSA Security Subgroup**, the guidance brings together a consolidated framework of Defence Security Requirements and sets out how the MoD's necessary security controls should be applied in research and development environments.

The material explains the security measures required when handling Defence Related Classified Material (DRCM) and offers practical support for managing risks throughout the research lifecycle. It is **intended for anyone involved in defence-related R&D**, including academic, administrative and commercial colleagues who may hold, manage or process sensitive material as part of a project.

The package includes:

- **MoD Research Worker Security Guide** – a quick-reference guide for individuals with authorised access to DRCM.
- **R&D Project Management Checklist** – a tool to help Lead Delivery Managers, including Principal Investigators, ensure that security considerations are addressed at the start of a project and maintained throughout.

The requirements reflect current legislative obligations as well as sector-specific considerations tailored to academic contexts. Institutions are encouraged to incorporate these measures into local policies, risk assessments, IT capabilities and training programmes to ensure consistent and proportionate security standards.

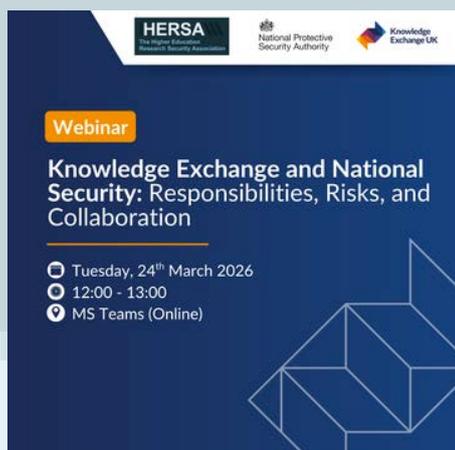
Significantly, the publication of this guidance is on a MOD GOV.UK page, which recognises the HERSA Security Subgroup's contribution and highlights a truly collaborative approach with DSTL and MoD to provide practical, impactful and effective security guidance.



HERSA and KE UK Webinar – 24 March, 12pm

We are collaborating with [Knowledge Exchange UK](#) to deliver a webinar, '**Knowledge Exchange and National Security: Responsibilities, Risks, and Collaboration**'.

Knowledge exchange helps ensure that new technologies and ideas achieve meaningful impact, often across international boundaries. Although the HERSA community is fairly familiar with the national security considerations linked to emerging and sensitive technologies, this collaboration with Knowledge Exchange UK provides an opportunity to extend awareness more widely and support colleagues across the sector.



HERSA
The Higher Education Research Security Association

National Protective Security Authority

Knowledge Exchange UK

Webinar

Knowledge Exchange and National Security: Responsibilities, Risks, and Collaboration

Tuesday, 24th March 2026
12:00 - 13:00
MS Teams (Online)

The webinar will introduce the key issues at the intersection of knowledge exchange and national security, and open a discussion about their implications.

The **webinar takes place on 24 March, 12.00-13.00** and is open to Knowledge Exchange UK members. Membership is held at an organisational level, so **contact the KE UK team if you are unsure of your organisation's status.**



New DfE Guidance: Protecting UK Higher Education from Foreign Interference

The [Department for Education \(DfE\)](#) has published new guidance on GOV.UK aimed at protecting UK higher education from foreign interference. It is designed to help providers recognise the risks, understand the different forms interference can take, and know when and how to report concerns.

The guidance focuses on three core areas: **responding to transnational repression**, **managing risks to individuals**, and **protecting higher education from cyber threats**. It also highlights how foreign interference intersects with wider agendas, including research security led by DSIT, and trusted research activity supported by NPSA and the NCSC.



MOD Announce £80m Student Skills Investment to Boost UK Defence

The Government has announced an £80 million investment to **expand student places on strategically important courses** that support the UK's defence and national security needs. Through the Defence Industrial Strategy, universities, colleges and other higher education providers in England will be able to bid for funding to increase opportunities for students on defence-related programmes. Work is also under way with the devolved governments to understand specific skills needs across the rest of the UK.

£50 million will fund around 2,400 new student places over the next six years, while a further £30 million will support improvements to university facilities, including new teaching spaces to expand capacity over the next decade. **Courses in engineering and computer science will be prioritised given their critical role in defence and national security.**

A new **Defence Universities Alliance** will establish a UK-wide network of universities working with the Ministry of Defence, Armed Forces and industry partners to support innovation and encourage graduates to pursue careers in defence-related sectors. **Intent to join the Alliance will be an important factor in grant decisions**, ensuring funded courses translate into real employment opportunities and help to meet long-term sector needs.



UK Vice Chancellors Receive Security Briefing

A joint update from the **DfE, Cabinet Office, Home Office, FCDO**, the **Security Service** and the **NCSC** highlighted a rare security briefing delivered to Vice Chancellors from across the UK earlier this month. **Senior leaders from more than 70 universities** attended the session, which was led by the MI5 Director General and the CEO of the National Cyber Security Centre.

The briefing examined how foreign interference can manifest in higher education, including attempts to influence research or teaching, and outlined the practical steps universities can take to recognise, resist and report concern.

The update comes alongside a £3 million investment in a wider package of measures aimed at supporting the sector. A new **Academic Interference Reporting Route** will allow senior university leaders to report concerns directly to government, enabling quicker action on individual cases and helping to build a clearer national picture of the threats facing UK institutions. **The DfE will also consult the sector on the design of a new proactive advisory service, supported by further guidance and training.**





Export Control Joint Unit: 2026 Upcoming Webinar Opportunities

The **Export Control Joint Unit (ECJU)**'s 2026 training opportunities are now available. While the in-person compliance and open licence workshops have already reached capacity, a series of pre-recorded webinars remains available to access, offering introductions to strategic export controls, licence applications and technology-related controls. 

The ECJU is also running several LITE Service Live webinars for exporters, covering topics such as applying for an Open Individual Export Licence (11 March), determining ultimate end users (24 March), editing applications (22 April), and understanding end users, consignees and third parties (14 May). 

Please note, the LITE Service webinars are general ECJU offerings and are not tailored or specific to the Higher Education context.

HERSA at ASCE 2026: Securing Knowledge Across Borders

HERSA is attending the 10th Annual **Academic Security and Counter Exploitation (ASCE)** Conference at Texas A&M University in the United States this week. Considered the world's largest gathering focused on research security, the ASCE Programme (led by the [Research and Innovation Security and Competitiveness Institute](#)) brings together more than 600 representatives from federal agencies, over 150 universities, and delegates from more than 25 countries.

This year's theme, '**Securing Knowledge Across Borders**', explores four areas: institutional research security; global collaboration and strategic partnerships; emerging threats and adaptive security approaches; and education, training, and workforce development in research security.

We look forward to sharing insights from the conference, including contributions to the international panel session! 



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 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.