

July 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

**NPSA Publishes Visitor Security
Recommendations for Universities**

**NS&I Act Annual Report 2025-26
Published**

**NPSA's 5 Principles for Building Org
Resilience Against Insider Risk**

**HERSA-EGADD U.S. Export Controls
Workshop Success!**

**Science Diplomacy: Sovereignty,
Strategy, and the Global Race**

**Austria Launches New Research
Security Resource Hub**

**U.S. DoW Releases Latest Section 1286
List of Foreign Research Institutions**

**U.S. NSF Publishes Update on
Upcoming Funding Restrictions**

NPSA Publishes Visitor Security Recommendations for Universities

Universities regularly welcome visiting academics, researchers, contractors, collaborators, and other guests whose contributions are vital to research and innovation. Ensuring visits are managed securely is equally important, **helping institutions protect people, information, assets and research** while maintaining an open and collaborative environment.

To support the sector, the **National Protective Security Authority (NPSA)** has worked with UK universities to develop **Visitor Security Policy Recommendations**.

The guidance provides **practical advice for managing visitors throughout the entire lifecycle of a visit**, from arrival through to departure and offboarding. It applies to a wide range of visits, including long-term research collaborations and one-off contractor visits, and covers areas such as visitor categorisation, host responsibilities, access management, and ensuring that access permissions are removed when a visit concludes.

Check out the guidance and see how it applies to your institution.



NS&I Act Annual Report 2025–26 Published

The Government has published the **latest annual report** on the operation of the National Security and Investment Act (NSIA), covering the period from 1 April 2025 to 31 March 2026. The NSIA is **designed to support global investment into the UK while safeguarding the most sensitive areas of the economy** in a secure, predictable, and proportionate way. It provides the Government with the oversight and powers to intervene where acquisitions could undermine national security.

The report provides detailed insight into how the regime is being used to assess acquisitions that may pose national security risks. **During the reporting period, 1,324 notifications were received, representing a 15% increase on the previous year.** Of the 1,220 acquisitions reviewed, 95.6% were cleared with no further action required, while 4.4% were called in for a more detailed national security assessment.

The Government issued **9** final orders during the year, with 8 acquisitions permitted to proceed subject to conditions and one acquisition blocked entirely. **Defence, military and dual-use technologies**, and **critical suppliers to government** continued to feature prominently among notified and reviewed acquisitions. For universities and research-intensive organisations, the report provides a useful overview of the UK's investment screening landscape and the sectors attracting the greatest national security scrutiny.



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.



NPSA's 5 Principles for Building Organisational Resilience Against Insider Risk

Recent convictions under the National Security Act have highlighted the risks that can arise when individuals misuse privileged access on behalf of a foreign intelligence service – while organisations often focus on external threats, **insider risk remains a significant and often overlooked challenge**. Insider risk encompasses the potential for harm or loss caused by the actions, whether deliberate or inadvertent, of individuals within an organisation.

The National Protective Security Authority's (NPSA) **Setting the Foundations Guidance** outlines **five principles** for developing a shared understanding of insider risk and strengthening organisational resilience:

1. Adopting a shared language
2. Broadening our understanding of potential insider threats
3. Considering the 'spectrum of intent', from unintentional to intentional insider activity
4. Detecting signs of and de-escalating insider risk
5. Establishing the foundations for effective interventions

Alongside this guidance, **NPSA's Insider Risk Mitigation Framework** provides a structured approach to developing an insider threat programme, helping organisations assess their security posture and implement proportionate, risk-based measures to reduce vulnerability. **Whether you are new to the topic or an experienced security practitioner, these resources offer practical insights into recognising, managing and mitigating insider risk.**



HERSA-EGADD U.S. Export Controls Workshop Success!

Earlier this month we welcomed colleagues to our **U.S. Export Controls Compliance Workshop**, delivered in partnership with the [Export Group for Aerospace, Defence & Dual-Use \(EGADD\)](#).

Delegates explored the practical implications of **International Traffic in Arms Regulations (ITAR)** and **Export Administration Regulations (EAR)** compliance, with the session covering topics relating to emerging and foundational technologies, U.S Gov contracts, sanctions, and challenges associated with intangible technology transfers, re-exports and dual/third-country nationals.

With thanks to [Squire Patton Boggs](#), [BAE Systems](#), and [ADS Group](#) for leading the session and for contributing their valuable time and expertise to this important topic.

Keep a look out shortly for further details on our plans to establish a **joint HERSA-EGADD industry and academia working group**, creating an ongoing forum for collaboration and knowledge exchange.



Science Diplomacy: Sovereignty, Strategy, and the Global Race

The **House of Commons Science, Innovation and Technology Committee** has published its report, **Science Diplomacy: Sovereignty, Strategy, and the Global Race**, which considers the UK's approach to science diplomacy in an increasingly complex geopolitical environment. The report argues that **rapid technological change, geopolitical instability, and shifting international alliances have made science diplomacy more important than ever**. It concludes that, despite ambitious objectives, the Government has yet to set out a coherent strategic framework defining its priority international partners, technology areas, and intended outcomes. The Committee **calls for a comprehensive science diplomacy strategy that aligns scientific collaboration with wider economic, security, and foreign policy objectives**.

The report also raises **important questions about technology sovereignty, research commercialisation, and research security** at a time when many UK universities are facing significant financial and operational pressures – while recognising the UK's strengths in science and innovation, it highlights ongoing challenges in scaling research into globally competitive businesses and retaining strategic capabilities. Notably, the Committee argues that **the Government's current 'actor agnostic' approach to research security has not translated into sufficiently clear or practical guidance** for the academics and institutions expected to manage these risks on the ground. The report suggests that **universities are being asked to balance openness, international collaboration and security considerations without a sufficiently clear framework, while simultaneously navigating wider structural challenges across the higher education sector**. It concludes that while the UK remains a global leader in both science and diplomacy, it lacks the explicit strategy and cross-government coordination needed to maximise the benefits of science diplomacy and protect national interests. **Read the full report.**



Austria Launches New Research Security Resource Hub

The [Austrian Federal Ministry for Innovation, Mobility and Infrastructure](#) has launched a dedicated research security section on its website, with the aim to improve awareness, support informed decision-making and strengthen knowledge exchange. The new resource hub brings together guidance and information from a range of sources, including European Commission materials, international initiatives, and publications from organisations working in research security.



U.S. DoW Releases Latest Section 1286 List of Foreign Research Institutions

The [U.S. Department of War](#) has published the Fiscal Year 2025 update to its [NDA Section 1286 List](#), identifying **130 academic and research institutions** in China, Russia, and Iran that it considers to be engaged in activities that increase the **risk of unauthorised technology transfer and the misappropriation of U.S. Government-funded research**. The list forms part of wider efforts to protect taxpayer-funded research, intellectual property, and national security interests.

From FY2026, the Department is prohibited from using funds for fundamental research involving collaboration with any entity on the most recent Section 1286 List, including the use of equipment from listed institutions. **Researchers, academic institutions, and industry partners are advised that collaborating with individuals affiliated with listed entities may pose a compliance risk and could affect eligibility for federal funding**, with recommendations for organisations to review any potential implications for existing or future partnerships.



U.S. NSF Publishes Update on Upcoming Funding Restrictions

The [U.S. National Science Foundation \(NSF\)](#) has recently published an open letter outlining a forthcoming policy that will prohibit the use of NSF funding for research conducted in collaboration with entities appearing on a range of [U.S. restricted party lists](#). The proposed approach consolidates a number of existing list-based controls and reflects a wider U.S. Government effort to protect federally funded research from national security risks.

Aligning closely with recent measures introduced by the U.S. DoW (above), under the NSF proposal, **NSF funds will not be available for grants, contracts, or other assistance where the purpose is to conduct research in collaboration with restricted entities**. The restrictions would also apply to employees of those entities, while senior or key personnel on NSF-funded projects would be prohibited from collaborating with, holding positions at, or receiving research support from restricted entities.

Organisations involved in U.S.-funded research may therefore wish to review existing partnerships and monitor further developments ahead of implementation, currently expected in FY2027.



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.