

# Monthly Membership Update

Post-Summer 2025



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

**NTE 2025/20: Updated End User Undertaking (EUU) and Guidance**

**Securing Converged Technologies: Insights from Subject Matter Experts**

**HEECA-ECJU Training Programme Impact Summary Report - Now Available!**

**Have Your Say: Compliance in Academia - Tools and Challenges**

**FIRS - First Public Register Entries Published**

**U.S. Dept for Education & U.S. NCSC Release 'Safeguarding Academia' Guidance**

**Coming Soon: Major Expansion of ASPI's China Defence Universities Tracker**

**ASPI's 'Shifting the Needle': Evolving Australia's Research Security**

**Canada Security Intelligence Service (CSIS) 2024 Public Report Live**

## UK & RoI



### NTE 2025/20: Updated End User Undertaking (EUU) and Guidance

The **Export Control Joint Unit (ECJU)** has issued an updated **end user undertaking (EUU)** form with new guidance, now aligned more closely with licence application questions in LITE, to ensure ECJU has the information needed to assess the full export journey of controlled items.

Key changes include acceptance of digital signatures and removal of the company letterhead requirement.

The updated EUU should be used immediately, with the previous version only valid if signed and dated on or before 1st September 2025.

Check out the full NTE 2025/20 on GOV.UK.



## Securing Converged Technologies: Insights from Subject Matter Experts

A new report, **Securing Converged Technologies**, authored by **Dr Andrew C. Dwyer** and **Mikaela Brough** and **funded by DSIT**, was published on 8th August. Drawing on insights from 20 subject matter experts, the report explores the socio-technical security risks and implications of technology convergence.

The study found that identifying future points of convergence and their cybersecurity impact remains challenging, with experts expressing low confidence in predicting outcomes. Convergence is shown to arise not only from technology, but also through markets, innovation ecosystems, everyday adoption and geopolitics.

The report notes that adversarial behaviour and everyday harms create new challenges for mitigating risks, making convergence harder to navigate. Crucially, it emphasises the need for active, long-term community engagement to manage convergence effectively, as short-term speculation offers limited value.

The full report is now available on GOV.UK.



## HEECA-ECJU Training Programme Impact Summary Report - Now Available!

Following the success of the **6-month training programme in collaboration with ECJU**, we are pleased to finally share that our **impact summary report** is now live!

The report highlights key outcomes from the initiative, which was designed to strengthen understanding of export control regulations across the higher education sector. It brings together key themes of delegate feedback, reflections on wider institutional impact and priorities for scaling and sustaining the programme.

Findings show strong engagement from participants and demonstrate that the training has significantly improved awareness of compliance requirements, while underlining the importance of continued dialogue between academia, government and industry to support the broader research security agenda.



## Have Your Say: Compliance in Academia – Tools and Challenges

At the upcoming 3rd **Erlangen** Conference later this year, Irene Barinaga-Rementeria Ramirez will join a panel exploring approaches to compliance and export controls in UK universities. To prepare, we are seeking input from our members to ensure the discussion reflects real experiences from across the sector.

We want to hear about the challenges you face, the support you receive, and the tools or approaches that have worked in your organisation. Your contributions will help demonstrate the realities of compliance in UK academia and highlight both barriers and opportunities for improvement.

**Please take a few minutes to share your perspectives via the short form.** Submissions are anonymous unless you choose to provide your details.



## Foreign Influence Registration Scheme (FIRS) - First Public Register Entries Published

The Foreign Influence Registration Scheme (FIRS) public register has now gone live with its first two entries, **both related to political influence activities**. This marks the beginning of greater transparency around arrangements entered into by individuals or organisations under the direction of foreign powers. The entries are now accessible to the public via the **official FIRS portal**.

Why not take a look and see how these initial cases are appearing? It's a real-time insight into how the scheme works and what kinds of activity are being disclosed.



## International



### U.S. Department of Education & U.S. NCSC Release 'Safeguarding Academia' Guidance

The **U.S. Department of Education**, in partnership with the Office of the Director of National Intelligence's **National Counterintelligence and Security Center (NCSC)** and other federal agencies, has issued new guidance to help universities protect their research. Released through the [Safeguarding Academia bulletin](#), the materials highlight growing foreign threats to academic institutions and provide practical strategies for mitigation.

The guidance covers risks linked to foreign talent recruitment programmes, overseas research collaborations, espionage activities, and cyber intrusions targeting sensitive projects. It outlines measures universities and individual researchers can take to safeguard work, including strengthening compliance processes and adopting best practice security protocols. Institutions are also encouraged to report suspicious activity to U.S. authorities to support wider national security efforts. The bulletin is accompanied by [reference guides](#) to help the academic community assess risks and implement protective measures.



### Coming Soon: Major Expansion of ASPI's China Defence Universities Tracker

Later this month, the **Australian Strategic Policy Institute (ASPI)** will release a major expansion of its widely used [China Defence Universities Tracker](#). Developed by ASPI's [Cyber, Technology & Security \(CTS\) Program](#), the Tracker is a global reference for governments, research institutions and companies assessing military, security and technology risks linked to Chinese universities and research bodies.

The update will add research on more than 50 institutions, including the Chinese Academy of Sciences and several joint venture universities and introduces new rankings on critical technology research, analysis of partnerships with Russian organisations, mapping of defence industry links and data on the growth of dual-use research centres.

From 2026, ASPI plans to roll out regular updates to further expand coverage and it is looking likely the Tracker will move to fee-based access. Stay tuned for the release.



## 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!



### ASPI's 'Shifting the Needle': Evolving Australia's Research Security

Earlier this summer, the **Australian Strategic Policy Institute (ASPI)** published a new report, [Shifting the Needle - Making Australia's Research Security Ecosystem Work Smarter](#), authored by **Brendan Munro**.

The report sets out Australia's comprehensive and globally recognised approach to research security, while noting that the threats facing the sector continue to evolve.

It argues that Australia's research security posture must also adapt, moving beyond a narrow focus on countering foreign interference and espionage, towards a broader, integrated and risk-based framework. The analysis highlights the importance of ensuring that policies remain agile and responsive to changing circumstances, enabling the research community to collaborate internationally while protecting sensitive work.

Explore the full report on ASPI's website.



### Canada Security Intelligence Service (CSIS) 2024 Public Report Live

The **Canadian Security Intelligence Service (CSIS)** has published its **Public Report 2024**, marking the agency's 40th year. The annual report provides an overview of the threat environment facing Canada and outlines CSIS activities over the past year. It highlights areas such as **espionage**, **foreign interference**, **terrorism** and **sabotage**, describing how the service is adapting its operations to address these challenges.

The report also sets out CSIS's role in supporting government decision-making and working with domestic and international partners. Readers can access the full document on the CSIS website.



## 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.