Membership Updates – July 2024

UK Government Baseline Personnel Security Standard (BPSS) Update Released

With the increasing desire for the UK Higher Education sector to engage and work with UK government on R&D activities through the likes of Dstl R-Cloud, HMGCC Co-Creation and ACE (Vivace), it's important to remain abreast of the changes associated with personnel security standards.

Check out the latest UK Government Baseline Personnel Security Standard (BPSS) (Version 7.0 – June 2024) now published, which forms as part of the Government Functional Standard GovS 007: Security, promoting consistent and coherent ways of working across government.

Why not join our **Security Subgroup** and play a key part in HEECA's role in supporting the sector understand and apply these requirements. Contact us at enquiries@heeca.org.uk to find out more information.

Increasing Awareness on Synthetic Biology (or Biosyn) in University Due Diligence Processes

In March 2024, we highlighted Synthetic Biology as a key area of significant interest to the UK government, particularly in relation to the National Security and Investment (NSI) Act.

In recent weeks, we have learned that UK universities are experiencing an increasing number of export licence refusals linked to this topic, noting some of projects (and project titles) do not have an obvious 'military' or 'dual use' link.

We encourage member institutions to reflect on their internal due diligence procedures to ensure that these types of projects are identified and assessed considering the broader research security regime.

New UK 'Cyber Security and Resilience Bill' Announced in the King's Speech

Announced in last week's King's Speech, the new Cyber Security and Resilience Bill aims to bolster the nation's defences against cyber threats by establishing stricter security measures and resilience protocols. Key provisions include enhancing the protection of critical infrastructure, improving incident response frameworks, and mandating higher security standards across public and private sectors.

The bill is a proactive step towards safeguarding the UK's digital landscape, ensuring robust protection against evolving cyber risks.

Read the full introduction in the King's Speech here.

Trusted Research and National Security: New Additions to UKRI Funding Terms

The standard terms and conditions for UKRI research grants have been updated, outlining UKRI expectations in relation to Trusted Research and National Security, for organisations in receipt of UKRI funding. These additions (RGC 2.7.1 and 2.7.2) can be found below:

RGC 2.7.1 *You may be required to provide UKRI with additional information about how you are managing considerations and risks relating to Trusted Research and Innovation, and engage in any subsequent risk assessment activities requested by UKRI. Any recommended mitigations identified through the risk assessment will need to be agreed and in place before the grant start date.*

RGC 2.7.2 *Clauses around national security must be included in all grant agreements – regardless of technology area or partners involved – to allow relevant ongoing support by UKRI. Where required and agreed, and in line with all relevant data protection legislation, we will consult appropriate wider technical agencies across HMG to provide further assistance and recommendation.*

Access the policy update in full here.

U.S. BIS Issues Guidance on Addressing Export Diversion Risks

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) has recently issued new guidance outlining the different steps that are taken in informing industry and academia about parties (beyond those identified on public screening lists) that present risks of diversion of items subject to BIS export controls to countries or entities of concern.

The guidance also outlines certain responsibilities companies and universities have to comply with BIS regulations, as well as additional steps they should take to mitigate diversion risks.

Access the full update here.

Italy Announces National Controls on Non-EU Listed Items

On 1st July, Italy announced the adoption of new national controls on dual-use items (goods and technology), joining France, the Netherlands and Spain in invoking Article 9 of EU dual-use Regulation (2021/821), in the implementation of their own respective national control lists.

The new national measures introduce controls on exports, brokering, and technical assistance services for three specific categories: Category 2 (Materials processing), Category 3 (Electronics), Category 4 (Computers)

Items include:

- Software for development, production and use of additive manufacturing equipment
- (CryoCMOS) integrated circuits
- Signal amplifiers
- Equipment for additive manufacturing of metal/aluminium components
- Extreme UV masks
- Silicon/germanium epitaxial materials, fluorides, hydrides, chlorides and silicon/germanium oxides
- Semiconductor development and manufacturing technology
- Semiconductor Scanning Electron Microscopes (SEM)
- Integrated circuit process design kits
- Quantum computers and related device (or component) development software and technology

The new requirements will come into effect upon publication in the Official Journal of the Italian Government - Gazzetta Ufficiale della Repubblica Italiana.

The full list of dual-use items (and associated technical specifications) included in the National Control List are available here (*official IT-EN translation not currently available*).

Decree of the Deputy Minister of Foreign Affairs and International Cooperation no. 1325/BIS/371 of 01-07-2024 available here (*official IT-EN translation not currently available*).

Access the EU Compilation of National Control Lists here.

White House OSTP Releases Guidelines for Research Security Programmes at Covered Institutions

The White House Office of Science and Technology Policy (OSTP) has recently issued new guidelines to governmental funding agencies, on the implementation of research security programmes at applicable research institutions. The release includes guidelines on implementing a certification requirement imposed by National Security Presidential Memorandum-33 (NSPM-33) – specifically, funding agencies must require certain research universities and federally-funded research institutions to certify that they have established and operate a research security programme.

Access the release here.

China Implements New Smartphone Inspections to Enhance Anti-Espionage Measures

Earlier this month, newly implemented regulations under China's counter-espionage law came into effect, granting authorities the power to inspect personal electronic devices, such as phones and computers, based solely on suspicion of espionage. This has sparked widespread concern on social media, with fears that foreigners and others may face these inspections when entering the country.

View the media release here.

U.S. BIS Settles Alleged Export Control Violations with Indiana University

Following a voluntary self-disclosure by Indiana University (IU), U.S. Bureau of Industry and Security (BIS) have issued an order imposing an administrative penalty on the university, regarding an alleged 42 violations relating to the export of fruit flies genetically modified to produce a subunit of a controlled toxin. These exports went to numerous research institutions and universities worldwide without the required export licenses.

IU cooperated with the investigation by BIS's Office of Export Enforcement (OEE), and took remedial measures after discovering the conduct at issue, which resulted in a significant reduction in the penalty.

Access the BIS release here.

[END OF DOCUMENT]