

Collaborative research: security and risk

Quick links:

National Security and Investment Act

Trusted Research

[Foreign Influence Registration Scheme](#)

Introduction

There has been an increased focus on national security involving research, engagement and research collaborations in the United Kingdom and abroad due to its risks. The UK Government has become increasingly aware of, and responsive to, the security risks around international collaboration, engagement and research, in particular where there are economic and security consequences. In response to these risks and challenges, there have been several new statutory and policy regimes introduced in the UK: the National Security and Investment Act 2021 (the NS&I), UKRI's Trusted Research and Innovation Principles 2021 (Trusted Research) and the Foreign Influence Registration Scheme (FIRS).

In line with LSE's Research for the World strategy, the guidance below aims to ensure that our research and the way in which researchers operate is conducted to the highest professional standards and meets regulatory requirements, to facilitate external research collaboration to strengthen research excellence and partnership opportunities.

A quick summary of each is set out in the table below, with more detail on each in subsequent sections.

Guidance and information about Export control is supported by the [LSE legal team](#) in the Secretary's division.

	National Security and Investment Act (NS&I)	Trusted Research	Foreign Influence Registration Scheme (FIRS)
Status	UK Government act	UKRI principles	Expected to come into force in early 2025
What does it cover?	Scrutiny of acquisitions including intellectual property (IP)	IP, sensitive research and its exploitation by external hostile actors	Political influence activities in the UK at the direction of a foreign power
What's required?	Notification to government in certain circumstances via online portal	Assessment of partner suitability; managing information and knowledge sharing; protecting commercial applications	Two tier registration process via online portal
How do we manage this?	Academic assessment; advice from R&I; Academic Unit and R&I	Academic assessment of risks; due diligence undertaken	Guidance will follow publication of the scheme

	collaborate on notifications		
How can I find out more?	National Security and Investment Act 2021 - GOV.UK (www.gov.uk)	Trusted Research NPSA	Foreign Influence Registration Scheme factsheet - GOV.UK (www.gov.uk)

For advice on any of the frameworks listed above, please email RI.Security@lse.ac.uk
Training will be provided by Research & Innovation.

National Security and Investment Act

What is the NS&I?

The [National Security and Investment Act 2021](#) (NS&I Act) came into force on 4th January 2022. Under the NS&I, the government can scrutinise and intervene in certain acquisitions made by organisations, including universities, businesses and investors, that could harm the UK's national security.

The NS&I allows the government to impose certain conditions on acquisitions occurring after November 2020, and in rare instances, to unwind or block an acquisition completely. This applies whether the acquisition has been completed or is still in progress or contemplation.

Any party acquiring a 'qualifying entity' (defined as any entity other than an individual) is legally required to tell the government if it falls into 17 sensitive areas that are more likely to give rise to national security risks. The 17 areas are as follows:

- Advanced Materials
- Advanced Robotics
- Artificial Intelligence
- Civil Nuclear
- Communications
- Computing Hardware
- Critical Suppliers to Government
- Cryptographic Authentication
- Data Infrastructure
- Defence
- Energy
- Military and Dual-Use
- Quantum Technologies
- Satellite and Space Technologies
- Suppliers to the Emergency Services
- Synthetic Biology
- Transport

How might this affect me?

The NS&I Act directly concerns the LSE with respect to acquisition of an interest in assets, which includes intellectual property rights. Although, as a social science institution there is a lower likelihood that the NS&I Act will impact LSE's acquisition of an entity due to the nature of our research, and its proximity to the 17 areas.

However, all LSE staff supporting and conducting research need to understand any ramifications of sharing LSE research outputs either informally or formally (e.g. collaboration agreements). Below is a list of scenarios of when intellectual property rights may need to be reviewed to ascertain whether a voluntary notification is required under the NS&I Act.

Licences and Assignments

For external licences involving third parties, a voluntary notification might arise likely in relation to the 17 areas for:

- a grant of a licence (whether it is an exclusive or non-exclusive licence)
- a licence which may confer an assignment of intellectual property rights
- an increased level of control over the intellectual property rights.

Internal licences to LSE staff, where a member of staff licences their intellectual property rights to LSE or where LSE licences its intellectual property rights to a member of staff, are unlikely to be of national security interest.

Collaboration and consortium agreements

Collaboration and consortium agreements between the LSE and a third party which may require control of intellectual property by a lead party.

Commercialisation

Creation of a spin out company where LSE will usually require an equity shareholding. The company will need to maintain its own internal exports control policy. As an equity shareholder, LSE will need to monitor the spin out company's operations from a NS&I Act perspective. However, the overall responsibility for a voluntary or mandatory notification will remain with the spin out company.

Other agreements

LSE's sponsored research agreements, gifts agreements where there is an assignment or licence of intellectual property rights, or consultancy agreements.

A voluntary notification will need to be considered where an existing agreement is either being revised (a variation) or rights therein are transferred to a third party (novation).

Where can I get more advice?

Research & Innovation will work collaboratively with you to identify and work through any potential activities which may come under NSI. Email RI.Security@lse.ac.uk in the first instance.

Trusted Research

What is Trusted Research?

Trusted Research is a cross government, cross research and innovation sector term for protecting the UK's intellectual property, sensitive research, infrastructure and its exploitation by a hostile state or other similar actors. It is concerned with potential security threats and risks to international collaborative research and innovation activities. The UK Government has created the [Trusted Research](#) guidance and service to help UK researchers and innovators protect the UK's intellectual property, sensitive research and its exploitation by external hostile actors. Trusted Research is mainly designed to highlight possible national, legal, financial and reputational risks as early as possible.

As a response, UK Research and Innovation (the UK's public funding body for research and innovation) established its [trusted research and innovation \(TR&I\) work programme](#) in order to:

- a) provide guidance to the sector about managing collaborative activities safely and securely; and
- b) minimise the risks UK may face within a global research and innovation ecosystem.

UKRI has published [a set of principles](#) about how to apply TR&I to new and existing UKRI grants. Organisations funded by the UKRI are required to adopt these principles and be able to evidence the controls and measures that have been put in place. The principles are:

- i. *Assessment of Partner Suitability*: appropriate due diligence assessment should be undertaken of potential collaborative partner organisations. These include factors such as the nature of the project activity, any envisaged outputs, dual project use (military or civilian use) etc. An assessment must take into consideration the following key issues:
 - a. Legal framework: collaborator's governing documents including any formal or informal affiliations with other businesses, government departments or military should be reviewed.
 - b. Values: democratic and ethical values, and how these may differ from the UK's values.
 - c. Conflict of interest: create awareness, in particular evaluation of any risks involving individuals who have interaction with LSE academics, access to organisation via employment, study, collaboration etc.
- ii. *Managing Information and Knowledge Sharing*
 - a. Cyber Security: development of robust cyber security control (prevention) and security awareness through training programs.
 - b. Separation of Data: sensitive data (including personal data) must be securely stored and, where a shared platform is used for information exchanged, data should be logically separated into different locations so it is only accessible by authorised individuals.
 - c. Access to Data: data access only granted to individuals with a clear requirement for access. It is important to understand whether there is any local (overseas) legislation which may allow for release of such data to local government institutions.

- d. Project Activity and Outputs: project activity and project outputs to be compliant with export control (including NS&I). Parties should be aware of any dual use and unethical application of the project outputs.
- iii. *Commercial Application*: appropriate agreements in place to ensure management of sensitive data and any intellectual property rights, particularly where there is future commercial use of the outputs.
- a. Intellectual Assets and Intellectual Property Rights (“IPR”): IPR should be managed in professional manner, including deciding when it is most appropriate to seek protection and subsequently how to exploit, assign, license or disseminate it to maximise its impact.
 - b. Publishing Project Outputs: all commercially sensitive outputs must be appropriately protected prior to publication, and should comply with UKRI’s open access policies once published.
 - c. Export Controls: an understanding of any relevant export controls which may apply to an organisation’s outputs and activities, including for any knowledge and technology transfer.

How might this affect me?

As a researcher, you should work with R&I to:

- Assess if your research is sensitive, including the assessment of commercial sensitivity
- Ensure your partners are suitable according to the Trusted Research principles
- Have due diligence checks done on research funders or collaborators you want to engage (which are usually done by using publicly available information)
- Consider the data and information sharing arrangements with your partners carefully
- Make sure you comply with UK regulations and Acts (specifically the [NS&I Act](#)), GDPR, other policies. Depending on your collaborators and their countries, check if you need to comply with their home country legal frameworks.

For more information

Read the Government’s [Trusted Research Guidance for Academia](#).

Use the **Trusted Research Checklist For Academia** to assess your international project’s risk levels which can be downloaded from the same link above.

Consult the Research Due Diligence Manager for help to run LSE’s due diligence checks on your partners and funding sources.

Foreign Influence Registration Scheme

What is FIRS?

The Foreign Influence Registration Scheme (FIRS) is a two-tier scheme aimed at strengthening the resilience of the UK political system against covert foreign influence and

provide greater assurance around the activities of certain foreign powers or entities that are a national security risk.

FIRS will require the registration of arrangements to carry out political influence activities in the UK at the direction of a foreign power. The enhanced tier of FIRS gives the Secretary of State the power to require registration of a broader range of activities for specified countries, parts of countries or foreign government-controlled entities where this is necessary to protect the safety of interests of the UK.

A “direction” is an order or instruction to act. This could also be delivered in the language of a request, but only where there is a power relationship between the person and the foreign power which adds an element of control or expectation, for example through a contract, payment, coercion or the promise of future compensation or favourable treatment.

How might this affect me?

Academic collaborations will only require registration if they involve political influence activities directed by foreign powers, or if activities are directed by a country or state-controlled entity that the Secretary of State specified in regulations because they believe greater transparency is necessary to protect the safety or interests of the UK. Registrations will be made through an online portal.

Even if registration is required, this will not mean that academic and research collaborations require approval before they can take place. FIRS does not prevent any activity from taking place. Providing the arrangements are transparent, related activities will proceed as normal.

The two tiers are explained below:

Political influence tier

- This tier will require registration of arrangements to carry out political influence activities in the UK at the direction of a foreign power.
- These arrangements will need to be registered within 28 days of being made with the foreign power.
- Political influence activities include communications to senior decision makers such as UK ministers (and ministers of the devolved administrations), election candidates, MPs and senior civil servants. It also includes certain communications to the public where the source of the influence is not already clear, and disbursement of money, goods or services to UK persons for a political purpose. To be registerable, this activity has to be for the purpose of influencing UK public life, for example, elections, decisions of the government or members of either House of Parliament or the devolved legislatures.

Enhanced tier

- The scheme also contains a power to specify a foreign power, part of a foreign power, or an entity subject to foreign power control, where the Secretary of State considers it necessary to protect the safety or interests of the UK. Use of the power will be subject to Parliamentary approval.
- This tier will require the registration of:

- arrangements to carry out any activities within the UK at the direction of a specified power or entity: the person making the arrangement with the specified body will be responsible for registration
- activities carried out in the UK by specified foreign power-controlled entities. In these circumstances, the specified entity (not a foreign power) will be responsible for registration
- Where appropriate, the government may narrow the activities requiring registration under this tier. This will allow the requirements to be tailored to the risk posed by the foreign power or entity being specified.

FIRS is expected to be launched in 2025: further information will follow in due course.