TRUSTED RESEARCH

Supporting risk-aware international engagement

Research & Impact Services

Presentation overview

- Know Your Research
- Know Your Partner
- Know Compliance Obligations

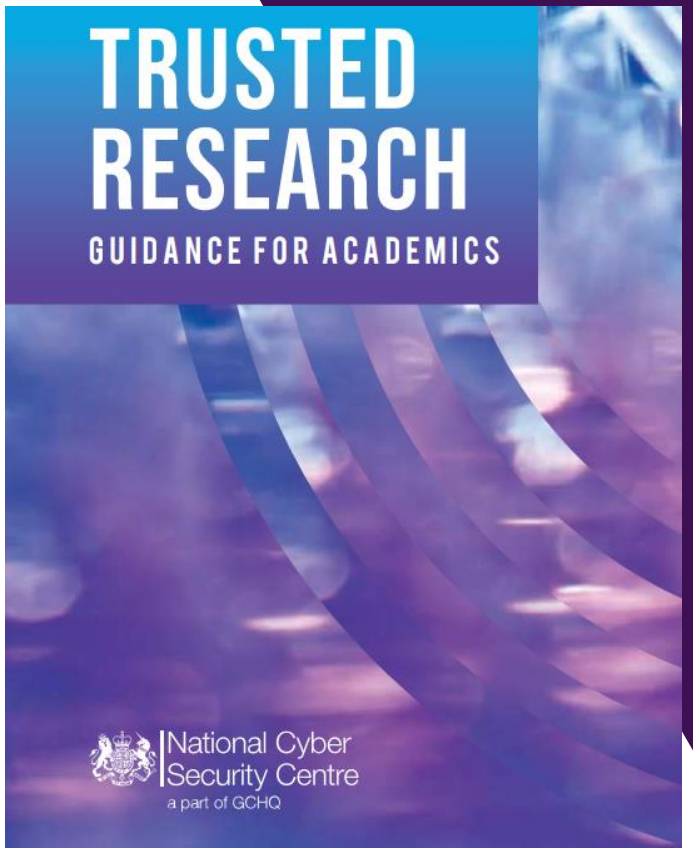
Context: Increased focus on international engagement risks

House of Commons

Foreign Affairs Committee

A cautious embrace: defending democracy in an age of autocracies

Second Report of Session 2019



Trusted Research

- Trusted Research Guidelines released in 2021 by UK Government
- Raises awareness of the potential **risks** to UK research
- Helps researchers, UK universities and industry partners **to have confidence in international collaboration** and **make informed decisions around potential risks**
- Seeks to **protect research, IP, and personal information** whilst ensuring that measures are **proportionate to support international engagement**

What are you at risk from?

National Protective Security Agency states:

- *"State actors are targeting UK universities to steal personal data, research data and intellectual property and this could be used to help their own military, commercial and authoritarian interests."*

Why protect your research?

- **Protect** research, data, IP, and commercially sensitive information and technology
- **Protect** individual reputation
- **Protect** national security
- **Prevent** the misuse of your research
- **Prevent** legal consequences (e.g. A breach of UK Export Controls can be a **criminal offence)**

Know Your Partner

Who is funding your research and who is your research partner? Consider:

- How much information about the partner or funder is available?
- How did the relationship start?
- Are there shared objectives and values for the research? Have you established why this prospective partner wants to work with you?
- What are the affiliations with other countries and entities (e.g. foreign militaries)?
- Are there any conflicts of interest?
- How does the country in which your prospective partner is from or based approach academic freedom and open science?

First steps: Do basic open source searches, (e.g. check UK Sanctions list), and engage R&IS for a due diligence assessment

Know Your Research

What are the potential uses of your research?

- Are you undertaking research collaboration in a sensitive area?
- Are there any dual-use applications to your research?
- Is any of the research likely to be subject to UK or other countries' export licence controls?
- Are there commercial applications of the research and are there IP protections in place?
- Do you need to protect sensitive data or personally identifiable information (e.g. genetic or medical information, population datasets, personal details, commercial test data)?
- Will your prospective partner be granted access to your institution's IT network? What wider visibility of your institution's research and data could this give them?
- **First steps: consider the potential uses of your research and engage RIS**

Sensitive research areas

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

Based on list from National Security & Investment Act

UK funders now require description of Trusted Research plan

Example question: *Describe what due diligence for ethical, legal, financial and security considerations have been undertaken in planning the project and how you will ensure physical and on-line segregation of data and outcomes from this project and other research project leaders are undertaking. (No more than 1000 characters including spaces)*

- **Other major funders, such as US funders, have similar requirements to consider how research and IP will be protected**
- **RIS can assist**

Case study : Collaboration with poorly known partner and undesirable technology and IP transfer

- You are a research leader in **robotics,** and you are seeking to develop research partnerships with academic and industry partners.
- A colleague (**Colleague A)** suggests to work with an individual that was a former PhD student (**Researcher A**) of another colleague, now a leading academic in robotics.
- You contact **Researcher A** in **Country X**, inviting them to be a visiting scholar for six months to develop research ideas and potential commercial applications of the research.
- **Researcher A** and you undertake a productive collaborative relationship publishing multiple papers in top journals and developing an IP application
- Six months later, after Research A has left the UK, a major newspaper publishes a story identifying **Researcher A**, reporting that **Researcher A** has transferred to IP to **Country X's military** to support military modernisation

Risks and mitigation options

Potential consequences:

- reputation damage to you and your institution
- limit your opportunities to win future funding
- Loss of economic and commercialisation opportunities
- National security risks

Potential steps to mitigate risks:

- Conduct proper due diligence on partner and their affiliations
- Engage with university IP and technology transfer team
- Export Controls assessment
- Ensure that the visiting scholar has an ATAS clearance

Source: NPSA Trusted Research resources

Case study: Risks while attending a conference

- As part of an ongoing research project funded by a UK funder, you attend an international conference to present your research in relation to increased **efficiency for aerospace engines**
- While at the conference, someone you have not met approaches you and starts to chat about your research. This individual proceeds to ask you meet their colleague.
- This colleague states they are looking to start a lab researching aerospace engines in Country X**,** and asks whether you would be willing to spend 2-3 months per year leading the lab in exchange for a cash payment, research funding, and 2 PhD students.
- ***What risks are present here? What steps could you take?***

Risks & mitigation options

Risks

- Export controls & national security risks
- Lack of IP protections
- Reputational damage
- Loss of commercial and economic opportunities

Mitigation options

- Due diligence on partner (e.g. which research institute/university or company are they affiliated with?)
- Export controls assessment
- IP protections

WARWICK
THE UNIVERSITY OF WARWICK

KNOW YOUR COMPLIANCE OBLIGATIONS FOR INTERNATIONAL ENGAGEMENT

“Export Control” refers to the regulations that control the sharing of sensitive items to individuals who are outside of the UK

Export-Control@warwick.ac.uk

Export Controls

- Prevent the proliferation of Weapons of Mass Destruction (WMD) and counter international threats including terrorism
- **Military, Dual Use, and Catch All** provisions

Export license may apply to 'Controlled'

- **Physical goods**: Samples, equipment, materials, parts, laptops, etc.
- **Technology and information:** Data, knowledge, know-how, etc.
- **Categories:** *Nuclear materials, facilities and equipment; Special materials and related equipment; Materials processing; Electronics; Computers; Telecommunications and "information security"; Sensors and lasers; Navigations and avionics; Marine; Aerospace and Propulsion*

<u>UK Legislation</u>

Export Control Act (2002)

Export Control Order (2008)

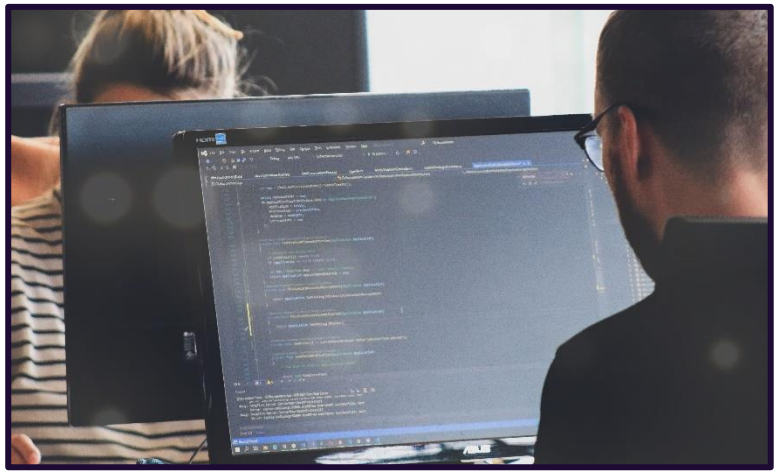
What is an Export?

The physical taking or sending of items outside of the UK:

- Shipping components/devices/samples to a collaborator, or for repair/maintenance
- Travelling overseas with an item (e.g., laptop, phone, memory stick, hard drive, camera)

The electronic transmission of items outside of the UK:

- Emailing information to overseas collaborators
- Technical discussions during an international web conference
- Digital / Remote Presentation
- Accessing data whilst outside of the UK (e.g., via cloud storage)
- Teaching overseas

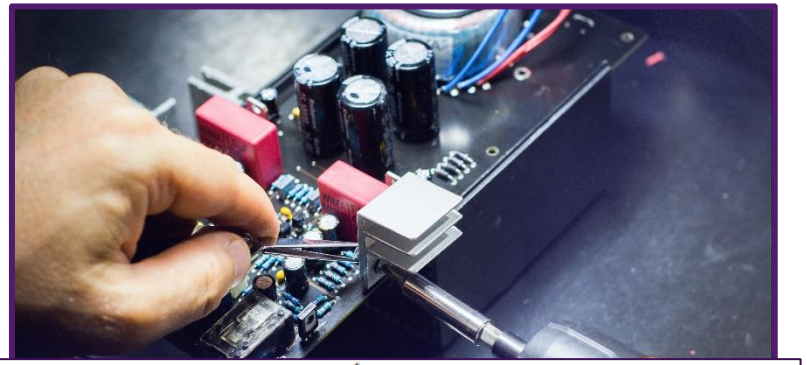


WARWICK

Defining Military and Dual-Use

Military

- **Specially designed** or modified for military use
- Design intent is key
- **NOT** just weapons



Dual-use

- May have a **military application** though not designed for that use
- Applies to **many goods** – from electronic components to raw materials
- Complex to interpret – based on **performance parameters**

- **Dual-Use List** [Annex I to Regulation (EC)[1] No. 428/2009]:
  - Category 0 Nuclear materials, facilities and equipment
  - Category 1 Special materials and related equipment
  - Category 2 Materials processing
  - Category 3 Electronics
  - Category 4 Computers
  - Category 5 Telecommunications and "information security"
  - Category 6 Sensors and lasers
  - Category 7 Navigation and avionics
  - Category 8 Marine
  - Category 9 Aerospace and Propulsion

Sanctions & Penalties

- A breach of UK Export Controls can be a **criminal offence**
- Sanctions apply to **individual researchers and institution**
- Accidental non-compliance followed by voluntary disclosure: **civil penalties**
- Knowingly exporting without a licence: **criminal offence**
- Unlimited fines
- Prison sentence up to a **maximum c**
- ❑ The Government produce an **Export** which details the number of fines in criminal sanctions

2020

- 19 compound penalties paid totalling £700,368.01. HMRC issued 19 co settlement offers ranging from £1,000 to £211,250 for unlicensed expo dual-use goods and related activity controlled by The Export Control Or

7.2 Enforce… Prosec…

HMRC continu… wide range of…

- 202 seizur… found to b…
- 122 end-u… brought w… put to an…
- 12 compo… compound… military goods, dual-use goods and related activity controlled by The Export Control Orde…
- 46 HMRC warning letters issued as a result of voluntary disclosures
- There were no strategic exports or sanctions prosecutions in 2021

Compound settlements

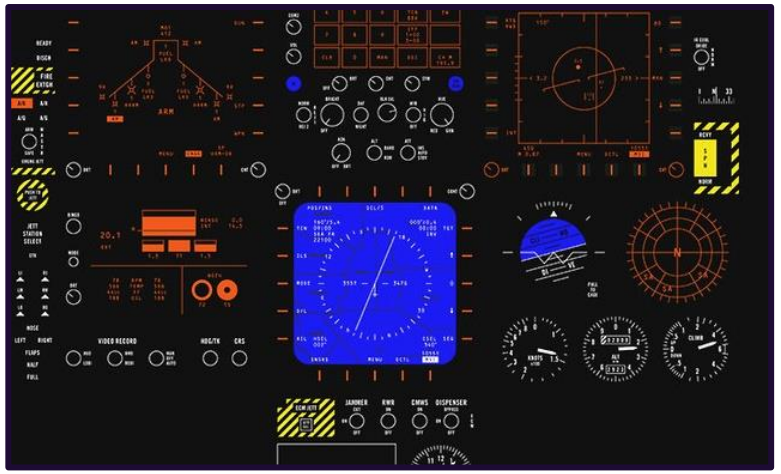
The 4 settlements made by UK companies were:

- in November 2022, £745,620.00 was paid relating to the unlicensed exports of … use goods controlled by The Export Control Order 2008
- in December 2022, £994,074.74 was paid relating to the unlicensed exports of military goods controlled by The Export Control Order 2008
- in December 2022, £1,000.00 was paid relating to the unlicensed trade in militar… goods controlled by The Export Control Order 2008
- in December 2022, £1,883,442.00 was paid relating to the unlicensed exports o… military goods controlled by The Export Control Order 2008

Export-Control@warwick.ac.uk

Defining WMD and Military End Use

Both apply to “non-listed” items



WMD end use

- You know, have reason to suspect or have been informed…
- That the end-use is for “WMD purposes”
- Includes defensive work (e.g., detection)
- Note – **WMD end use controls transfers within the UK!**

Military end use

- You know or have been informed…
- That the end use is “military in the recipient’s country”
- Only apply to destinations subject to subject to arms embargo

WARWICK

Two Exemptions for Academic Research

Basic Scientific Research

- be solely to add to the sum of human knowledge
- not be aimed at a specific (short-term) practical aim
- not address a specific technical problem

Consider the Technology Readiness Level (TRL) - <3 would be BSR

Only applies to dual-use technologies

In the public domain

Information that is already in the public domain can be shared freely without restriction.

Key University Compliance Processes

- **Research Grants and Contracts / Ethics and Sponsorship / Internal Funds**
  - Export control questions embedded into Ideate, Application Forms and NoI processes
  - Triggers a discussion with the Export Control Team

- **International Travel / Local Screening Processes**
  - University guidance issued circulated and questions are embedded in travel authorisation forms
  - Travel guidance added to the Institutional Policy

Both of these processes embed the same set of triaging questions

Key questions:

- Working with non-UK military organisation?
- Does work fall within any categories in control list?
- Could the “technology” or materials support the design, development, production, stockpiling or use of nuclear, chemical, or biological weapons?
- Do you have concerns about the end user?

What happens if the materials / equipment / "technology" I am working with is 'controlled'

If you determine that your research is 'controlled', this is not necessarily a roadblock!

- R&IS will support you to ensure that **the appropriate export licence is in place**.
- Contact **researchcompliance@warwick.ac.uk**, who will support you:
  - Identify relevant control list entry, or confirm end-user concerns.
  - Collate information and documentation for licence application.
  - Submit and manage licence application.
  - Provide instructions on compliance with licence terms.
- **Items and / or technology must not be exported until a licence is obtained.**

Example: Battery Technology

Research into battery technology can be subject to export controls

There are **three** primary ways in which battery technology can be captured by the regulations

WARWICK

Control Risk 1

1. Technology for the development / production / use of high energy density cells captured by control listing ***3E001 in relation to 3A001***.e.

3A001 [W] Electronic items as follows:

a. … b. … c. … d. …

e. High energy devices as follows:

1. 'Cells' as follows:
   a. 'Primary cells' having any of the following at 20°C;
      1. 'Energy density' exceeding 550 Wh/kg and a 'continuous power density' exceeding 50 W/kg; or
      2. 'Energy density' exceeding 50 Wh/kg and a 'continuous power density' exceeding 350 W/kg; or
   b. 'Secondary cells' having an 'energy density' exceeding 350 Wh/kg at 20°C;

3E Technology

3E001 "Technology" according to the General Technology Note for the "development" or "production" of equipment or materials specified in 3A, 3B or 3C;

Control Risk 2

2. Technology for the development / production / use of batteries that are **specially designed or modified for military application**

ML11 [M-**5**]	Electronic equipment, "spacecraft" and components, not specified elsewhere in this Schedule, as follows: a. Electronic equipment specially designed or modified for military use and specially designed components therefor;

Control Risk 3

3. Technology for the ‘development’ / ‘production’ / ‘use’ of batteries that are a specially designed component of **another listed ‘dual-use’ item.**

For example, batteries that are designed as a component of a detector controlled by 1A004c:

1A004 [W] Protective and detection equipment and components, not specially designed for military use, as follows:

N.B. SEE ALSO MILITARY GOODS CONTROLS, 2B351 AND 2B352.

a. … b. …

c. Detection systems, specially designed or modified for detection or identification of any of the following, and specially designed components therefor:

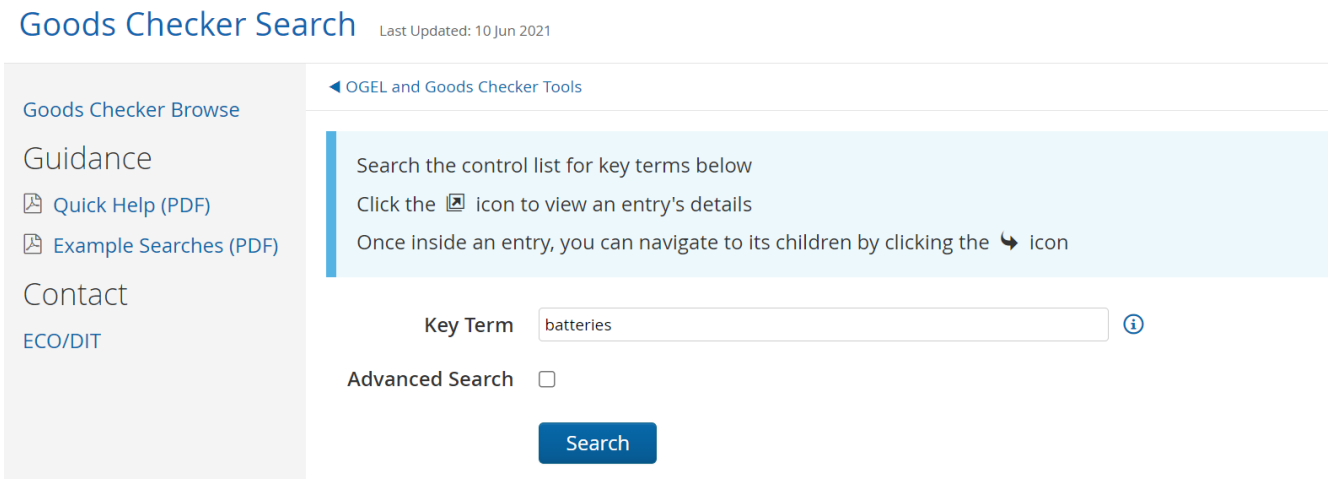
1. "Biological agents";
2. 'Radioactive materials'; or
3. Chemical warfare (CW) agents.

WARWICK

Key resources: Goods and OGEL Checker

Goods Checker: The Goods Checker Tool helps to establish if your items are controlled and identify the appropriate control entry ('rating') from the UK Strategic Export Control Lists.

OGEL Checker: The OGEL Checker helps to identify if an appropriate Open General Export Licence (OGEL) exists.



National Security & Investment Act

- Grants the government the right to **scrutinise, intervene, block, or unwind certain acquisitions** by UK and foreign entities, including universities, businesses, and investors, that could harm **the UK's national security**.
- **Relevant Qualifying entities (mandatory notification)** include universities, university subsidiary, and university spin-outs
- **Qualifying assets (non-mandatory)** include designs, plans, drawings and specifications, software, trade secrets, databases, source code, algorithms, formulae, land, tangible moveable property (e.g. lab equipment)

Notifications required in 17 critical areas: Advanced Materials, Advanced Robotics, AI, Civil Nuclear, Communications, Computing Hardware, Critical Suppliers to government, Cryptographic Authentication, Data Infrastructure, Defence, Energy, Military & Dual-Use, Quantum Technology, Satellite and Space Technologies, Suppliers to the Emergency Services, Synthetic Biology, Transport

Case study: National Security & Investment Act – compulsory notification

- Researchers at a UK university have developed a **new software system for autonomous vehicles** and are seeking to create a spin-out company.
- The spin-out company is seeking commercial partners to support the testing and manufacturing of vehicles with the new software.
- An overseas transport corporation (**Corporation A**) offers to invest funds in exchange for a ***25 % stake*** in the spin-out company.
- **Likely to require notification to UK government as the spin-out is in a critical area (transport) and gives Corporation A certain level of control over spin-out**
- **Dual-use and national security risk:** use of autonomous vehicles in defence settings
- High commercial value

Due Diligence

- Ensure the **integrity and reputability** of international partnerships
- Important to consider the **reputation** of proposed partner and funder
- **R&IS will undertake a risk assessment of collaborating with any international or national partner(s).** This will consist of gathering and reviewing prospective partners' financial, scholarly, professional and personal interests.
- Due diligence is undertaken on all partners/ collaborators on a research project. This applies irrespective of:

    1) whether they are project leads and

    2) whether they are international or UK-based.

Academic Technology Approval Scheme

- ATAS is a certificate issued by the Foreign Commonwealth and Development Office (FCDO) which gives you **security clearance to study certain subject areas** in the UK.
- These subject areas relate to where the knowledge gained may have an application in the **development or delivery of weapons of mass destruction**, for example, certain science subjects such as mathematics, engineering, technology or medicine.
- ATAS certification **required for visiting scholars and students**
- **You can check ATAS eligibility requirements-** Following countries are exempt:
- *Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, United States of America*

Key messages

- Trusted Research seeks to raise risk awareness while supporting international engagement
- Know Your Partner
- Know Your Research
- Know Your Compliance obligations
- Contact Research & Impact Services if you have any questions

Contact Details and Further Information

Research & Impact Services

Research & Impact Services International Research

National Security Protective Authority

Trusted Research Guidance for Academia

Questions?

THANKS