CPNI
Centre for the Protection of National Infrastructure

TRUSTED RESEARCH

GUIDANCE FOR INDUSTRY

National Cyber Security Centre
a part of GCHQ

The UK has a thriving research and innovation sector that attracts investment from across the world. More than half of UK research is a product of international partnerships. **Trusted Research** aims to secure the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector.

TABLE OF CONTENTS

INTRODUCTION

TRUSTED RESEARCH

Trusted Research is a campaign to raise awareness of the risks to research collaborations which may occur when working with organisations or research partners with links to nations whose democratic and ethical values are different from our own. This advice has been produced in consultation with academia and industry, and is designed to help the UK's world-leading research and innovation sector get the most out of international collaboration whilst protecting intellectual property (IP), sensitive research and personal information.

This guide is to assist industry in forming long-term, trusted and secure relationships with academia which are valued by both partners.

Trusted Research:

- Outlines the **potential risks** to UK research and innovation
- Helps researchers, UK universities and industry partners to have **confidence in international collaboration** and make **informed decisions** around those potential risks
- Explains how to **protect research** and **staff** from potential theft, misuse or exploitation

Industry and research

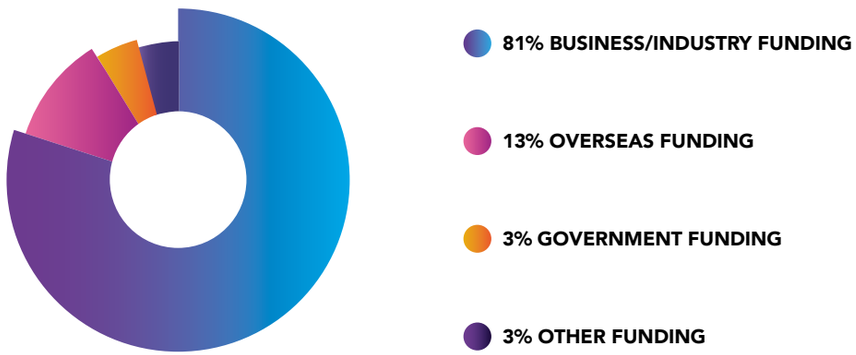
The business sector is the single largest contributor to UK research and development (R&D), spending £23.7 billion in 2017 and accounting for 68% of the total UK R&D expenditure. Expenditure on research and development performed by UK businesses reached £25.0 billion in 2018, an increase of 5.8%.[1]

The UK government's Industrial Strategy sets out a target to "raise investment on R&D to 2.4% of GDP by 2027". As the largest contributor to total UK R&D expenditure, the business sector is integral to achieving this objective.[2]

For industry, working with academia provides considerable benefits, such as access to high-quality research talent and facilities. Many industries and businesses innovate internally. However, it can be more efficient to sponsor academic research and may produce better research outcomes.

International trade and collaboration are essential to the continued prosperity of the UK. The government, through its Industrial Strategy and Export Strategy, seeks to support organisations of all sizes to take advantage of the opportunities offered through trading and collaborating across the globe. Trusted Research for Industry outlines how industrial partners can support academia to enable international partnerships to flourish and develop securely, safeguarding UK prosperity.

CIVIL R&D FUNDING



Civil R&D is primarily funded by business/industry (81%), with 13% from overseas funding and 3% from the UK government.

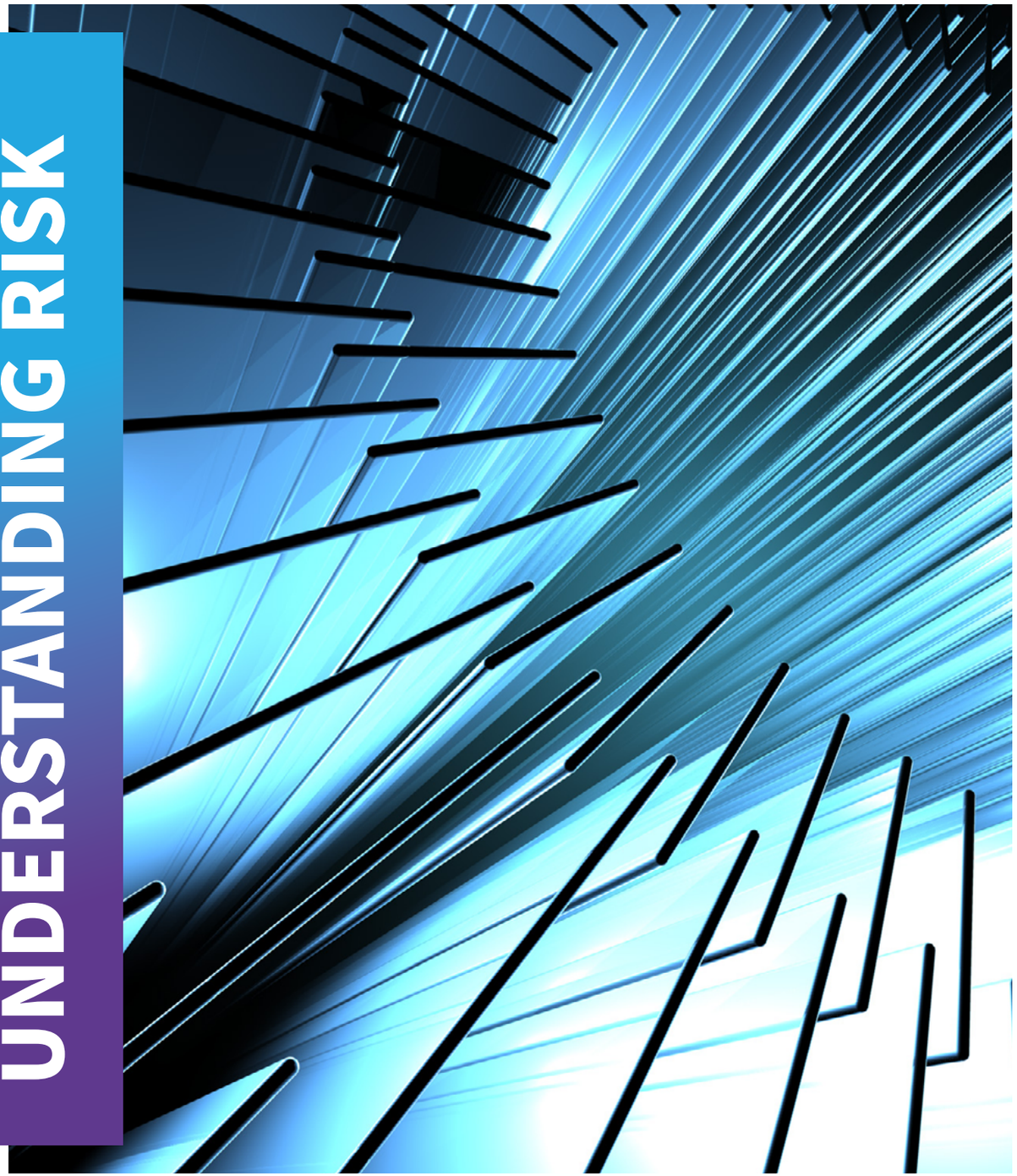
UNDERSTANDING ACADEMIA

More than half of UK research is a product of international partnerships and these international relationships extend further than collaboration; 42% of postgraduates and 31% of staff in universities are from outside the UK.[3]

Developing and maintaining these international relationships is key to the success of UK research and innovation and to the continued prosperity of the UK. Academic institutions are likely to have different motivators and drivers to a commercial company. Universities are constituted in a variety of ways; they often have charitable status, and many receive public funding for research and teaching. This means that the institution may have to identify a public good in the work that they undertake and be open and transparent about how they allocate resources. Individual academics will also want to publish their research in order to build and develop their academic reputation, for the purpose of peer review and to contribute to the global body of knowledge in their field.

1 Office for National Statistics, Business enterprise research and development, UK: 2018
2 Ibid.
3 Ibid.

UNDERSTANDING RISK



WHAT IS THE RISK TO YOUR ORGANISATION?

Having your research, IP or data compromised could result in damage to the reputation of your people, organisation or even the nation. Depending on the sensitivity of your research, it can also lead to legal proceedings and criminal prosecution.

What is considered high risk for your organisation will depend on your risk assessment and appetite. Your risk assessment should be carried out early and reviewed often.

HOW MIGHT YOUR RESEARCH INTERESTS BE TARGETED?

A hostile state is one whose democratic and ethical values are different from our own and whose strategic intent is hostile to the UK.

Hostile states are targeting UK universities to steal personal data, research data and intellectual property[4] and this could be used to help their own military, commercial and authoritarian interests.

International collaboration offers hostile states the opportunity to benefit from research without the need to undertake traditional espionage or cyber compromise. Collaboration can provide access to people, IT networks and participation in research which may be sensitive or have sensitive applications.

Traditional academic engagement provides an easy route for a hostile foreign intelligence service to gain access to academics, for example at a conference or research placement.

Universities and individual academics might also be targeted through a cyber attack, such as a phishing email, which might try to trick them into revealing sensitive information or contain links to a malicious website or infected attachment.

[4] https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities

HOW TO PROTECT YOUR RESEARCH

A STRATEGIC APPROACH

Investing time and resources into selecting the appropriate research partners and building secure, successful and long-term research relationships can be critical to the security of your research. If your organisation has a large portfolio of research relationships, it is good practice to periodically review your research strategy and partners.

IDENTIFY YOUR SENSITIVE RESEARCH

It is critical that you have a good understanding of what research you are undertaking with academic institutions and consider which are the most sensitive or important aspects of that research portfolio.

The first step is to consider which aspects of your existing and planned portfolio of research are critical to your future business model. Technology Readiness Levels (TRLs) could be a useful starting point to form an assessment of what is most sensitive within your research portfolio. TRLs are a method for estimating the maturity of technologies and how close they are to commercialisation.[5]

In forming this assessment, you might consider the following questions:

- What is the TRL of the research that you are conducting?
- What data or background IP are you sharing as part of the work and how sensitive or important is this to your business?
- What level of access to your company and IP is required for the research to be a success?
- What proportion of the funding for the project are you providing? This may influence your commercial arrangements with your partner or affect how any output from the research is disseminated.

[5] Mihaly, Heder (September 2017). "From NASA to EU: the evolution of the TRL scale in Public Sector Innovation" (PDF). The Innovation Journal. 22: 1–23. Archived from the original (PDF) on October 11, 2017

KNOW YOUR PARTNERS

When selecting your academic partners, you will want to consider their expertise and track record in the particular field of research that you are undertaking, their reputation, facilities and their past history of working with you. You should also consider their cyber maturity, including how they protect data from theft, how they control access and how they monitor the environment used for research.

There are different sources of information about the nature of academic partnerships. These range from basic open source searches through to commercial due diligence companies. This broader approach to due diligence can provide context to discuss how the university or academic could manage potential conflicts of interest.

Basic open source research can:

- Allow you to map out any competitors who may be engaged in similar research with your prospective or existing research partners
- Provide a better understanding of your partner's relationships with universities in countries who have different ethical and democratic frameworks to our own or universities who have close connections to state or military institutions overseas

CONCENTRATION VS DIVERSIFICATION

The most appropriate strategy for your research portfolio will depend on the nature of your business and the sensitivity of your research. Some organisations may seek to mitigate any risk to the "crown jewels" of their intellectual property or research data, by working with a range of research partners, ensuring that none of them has full access to the entirety of the data or research.

An alternative approach could be to use framework agreements with a small number of strategic partners. This allows investment into supporting those partners and developing longer term relationships. In such relationships, academia may also be more focused on protecting the resulting outcomes of the research and have the opportunity to develop a greater awareness of the potential threats to that research. Longer term, sustainable funding provides academic partners with greater confidence, allowing them to focus their attention on the protection of research rather than securing future funding.

Universities will want to work with a range of organisations, and it is unrealistic to expect research institutions not to work with your competitors. If a university is conducting research in the same field or even a closely related field for two competing organisations, you may wish to explore how they intend to segregate the respective research work.

Framework agreements

The purpose of this guidance is not to provide legal or contractual advice but to help highlight those areas that you might want to seek to protect.

Framework agreements are often brokered with university administrators, rather than individual departments, research groups or faculties. This poses the potential risk of individual academics or departments unknowingly breaching the terms of the agreement.

To mitigate this risk, you can:

- Ensure that your research partners are aware of their corporate contractual responsibilities
- Consider an education or training programme for researchers and staff working on your research programmes as a condition of your framework agreement
- Consider providing additional training to your own (industry) staff as many may not have experience of commercial, contractual or security matters

INTELLECTUAL PROPERTY

Some of the research that you are conducting with universities and research partners will result in the creation of IP. In order to protect that IP you may want to consider the following:

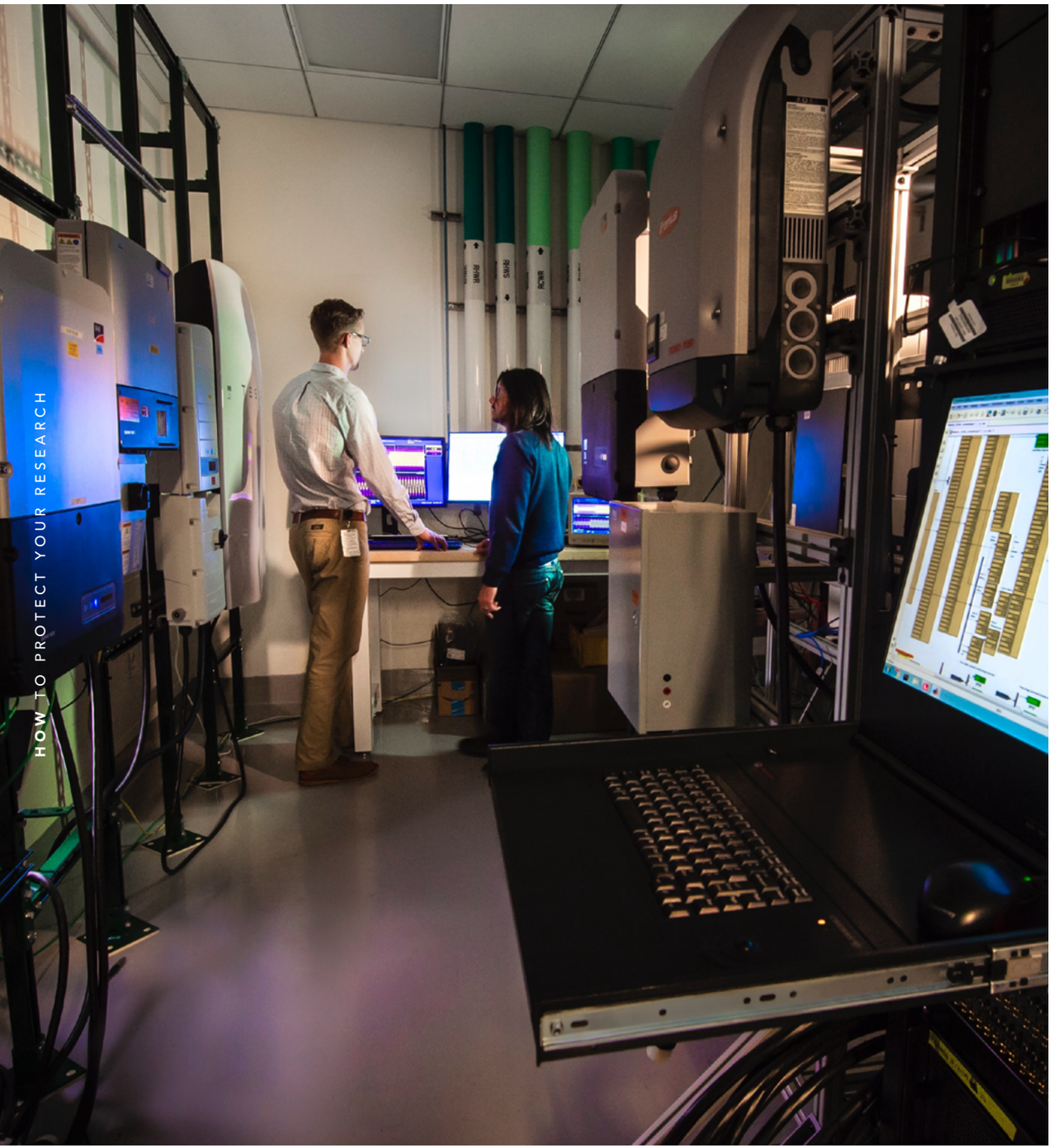
- What background IP are you providing to the project and how will this be protected?
- What are your requirements around the ownership of any resulting IP?
- What agreement do you have regarding the foreground IP produced from the research and likely ownership of that IP?
- Is the ownership of IP linked to the level and proportion of funding that you have contributed?

The UK Intellectual Property Office (IPO) designed the Lambert toolkit to assist academic or research institutions and industrial partners who wish to carry out research projects together. To find out more about the toolkit, please see the Further Information section.

PROTECTING YOUR INTELLECTUAL PROPERTY

Many companies and organisations will have a process for identifying or marking the level of sensitivity of their information, data or IP. Whatever system you deploy, it is helpful to make clear distinctions between high, medium and low levels of sensitivity. This can be particularly helpful in a research context where you are sharing background IP or data.

It may be helpful within any framework agreement to set out your expectations for how the different types of information that you may share with academic partners will be treated and protected.



PUBLISH AND PROTECT

In order to support trusted relationships with academia, it is vital to have a fair and proportionate approach to publishing.

Freedom to publish is an important aspect of academia and supporting academic partners to publish their research presents a non-financial incentive to motivate research excellence. It is entirely possible to support academic publishing whilst protecting research which is sensitive or may have commercial applications.

You may wish to consider:

- Specifying what constitutes publication
- An agreed arbitration process with your academic partner in order to manage sensitivities around publishing
- A contractual expectation that you will be consulted prior to publishing
- Identifying specific areas that may be redacted whilst allowing the overall content to be published
- Introducing time-bound access restrictions to the published material and delaying the publishing of research to allow for a patent application or a more advanced stage of commercialisation
- Setting requirements in relation to the publication of company confidential material, national security and export control

It is also vital to ensure that any disputes over sensitive areas of publication are resolved in a timely manner, including an agreed escalation process for any disputes. In most cases formal arbitration can be avoided by a pragmatic approach.

STRATEGIC REVIEW CHECKLIST

- Ensure that you regularly review the sensitivity of your research, and regularly audit your research partners
- Take a strategic approach to your research portfolio
- Consider framework agreements with your strategic partners which will ensure clear expectations for all projects rather than trying to agree them separately for each project
- Have clear and agreed expectations with your academic partners which reflect the needs of both parties

PROTECTING PEOPLE

Conflicts of interest

Many universities allow their staff time to undertake external work outside their normal academic duties, including writing articles, commercially funded research, consultancy work or overseas lecturing and presentations. Most will set an expectation that this ought not to conflict with their responsibilities to the university. It may be helpful to provide clarification through your contract or agreement with the university, outlining your understanding of what constitutes a conflict of interest. You may also wish to consider whether individual researchers working on your projects have a responsibility to notify you or seek agreement, especially when undertaking external work within the same or a related field of research.

CONFLICTS OF INTEREST IN THE RESEARCH SECTOR

In January 2020, the US Department of Justice announced the indictment of a prominent US academic for an alleged failure to disclose significant foreign financial conflicts of interest, including "financial support from foreign governments or foreign entities". The academic involved was alleged to be a participant in an overseas "talent programme" and was being paid $50,000 USD per month by an overseas university, and was awarded more than $1.5 million to establish a research lab at the university. At the time the academic was in receipt of $15,000,000 in grant funding from the National Institutes of Health (NIH) and Department of Defence (DOD). These grants require the disclosure of significant foreign financial conflicts of interest, including financial support from foreign governments or foreign entities.[6]

[6] https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related

Cyber security for research collaboration

It is highly likely that research collaboration and communication between all involved parties will rely on local and internet-based technologies. It is therefore imperative that cyber security is effectively applied to mitigate any associated risks.

The following section details some of the key areas that need to be considered in every type of collaboration. However, it is highly advisable to look at the cyber security advice and guidance developed by the National Cyber Security Centre (www.ncsc.go.uk) to ensure that you are aware of guidance specific to your situation and use of technology.

You may wish to encourage your research partners to think about implementing the following measures:

ACCESS CONTROL

It is important that you control access to sensitive data, whether that is personal data or research data. You should only allow users and partners with a valid requirement to have access to sensitive data, research and other parts of your networks.

You should also ensure that you understand the security of any collaborative IT platforms, especially those used by third parties.

UNAUTHORISED ACCESS MONITORING AND PREVENTION

Even when critical or highly sensitive data is separated and privileged access is limited, there may be instances of unauthorised access attempts. These could be from system users (insider threat) or from partners or other sources (external threat).

You should ensure there are effective cyber security arrangements in place to monitor and defend against unusual or malicious network activities.

SUPPLY CHAIN OR PARTNER ORGANISATION SECURITY

Understanding the security practices of partner organisations or managed service providers is vital in managing any issues they present. In particular, working with overseas organisations may present different legal and operational environments that could equate to higher levels of risk and mitigations different from those implemented for organisations operating in the same jurisdiction. You should develop an understanding of the cyber risks associated with partner organisations, managed service providers and potentially vulnerable components at an early stage.

You may also wish to confirm whether an institution is recognised as cyber security industry standard, in line with the NCSC's Cyber Essentials, as this will demonstrate that your partner is working to secure your research against a whole range of the most common cyber attacks. Guidance on these topics can also be found in the Further Information section.

SUPPORTING YOUR PARTNERS

ENGAGING WITH YOUR RESEARCH PARTNERS

After the initial selection of a research partner, it is important to remain engaged with them and, if possible, provide ongoing support in relation to the security of your research. It is advisable to continue to maintain visibility and awareness of any new research relationships that the university, or research institute, is considering which may present a conflict of interest. Establishing opportunities to encourage academic partners beyond pure financial support helps generate long-term trusted relationships. Within individual projects you may wish to meet regularly and discuss security-related issues.

A SECURITY-MINDED AGENDA FOR RESEARCH PARTNERS

A university with long-established industry relationships saw that having regular interactions with their partners was critical to their success. These occurred on a quarterly basis and they ensured that security was a standing item for discussion. When it came to publishing, they had an agreement with their sponsors that they would consult on the content of papers and have a set process for arbitrating any conflicts.

As the sponsors were engaged in a long-term funding relationship, there was an opportunity to consult early on new areas of research. These early discussions provided an opportunity to give confidence to the long-established industry partner.

The open and transparent relationship included discussing researchers working on a project, changes to personnel, and any visiting research fellows working on closely related topics. This ongoing dialogue extended to IT/network security and data protection and provided an opportunity to discuss how the sponsor's data and information was protected and held.

ROLES AND RESPONSIBILITIES

Having an academic partnership manager who is responsible for nurturing your academic partnerships and protecting the resulting research could be a means to ensure that your research collaboration is successful. You should ensure that those within your organisation are aware of the threat and mitigations that you have placed within framework agreements. Your staff should also be aware of the constraints and challenges within academia.

Whilst some of the advice in this guidance focuses on protecting against competitors in the same research area, there are instances in which competitors have a co-operative approach to working with and supporting academia. Working together can be a particularly effective way of helping to develop and nurture research and innovation within your partner institutions. In some cases, small minority share investments in research, particularly at an early stage, are an effective means of supporting academic partners as well as helping generate innovative new ideas and concepts which may provide new opportunities for future commercialisation.

TRAINING AND INFORMATION

It is also worth exploring opportunities to support the provision of training on IT security, confidentiality, physical security and IP protection for all staff working with you. Industry partners will have a good awareness of legal compliance in areas such as export control and the International Traffic in Arms Regulation (ITAR). Supporting your academic contacts with advice and training if they are less familiar with their obligations in these areas may be a good opportunity to build mutual collaboration.

RESEARCH REFRESHER

- Identify a strategic approach for your research portfolio
- Set clear expectations for your academic partners
- Discuss security issues as part of a regular review of research partnerships and individual projects
- Identify a proportionate balance between commercialisation of IP and academics' motivation to publish the results of their research for scientific review and validation
- Consider a framework agreement with your academic partners, which includes a fair agreement on the ownership and use of intellectual property
- Work with partners to help them to publish research in a manner which does not jeopardise future research opportunities and commercial exploitation
- Be visible and supportive to your academic partners
- Educate your own staff on the risks and opportunities of working with academia and involve them in engagement with the sector

FURTHER INFORMATION

Please see the following websites for more detailed information on the advice in this document:

CPNI and NCSC websites

www.cpni.gov.uk
www.ncsc.gov.uk

Guidance

Risk Management: www.ncsc.gov.uk/collection/risk-management-collection

Identity and Access Management: www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

Collaborative IT Platforms: https://www.ncsc.gov.uk/collection/saas-security

Cloud Security: www.ncsc.gov.uk/collection/cloud-security

Security Monitoring: www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

Supply Chain Security: www.ncsc.gov.uk/collection/supply-chain-security

Security Operation Centres: https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide

Phishing: www.ncsc.gov.uk/collection/small-business-guide/avoiding-phishing-attacks

Secure Business: www.cpni.gov.uk/secure-business.

Passport to Good Security: www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport.

Protective Security Risk Management: https://www.cpni.gov.uk/rmm/protective-security-risk-management.

https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgrossdomesticexpenditureonresearchanddevelopment/2018

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801513/International-research-innovation-strategy-single-page.pdf

Department for International Trade Export Control Joint Unit (ECJU)

Your Technology Transfer Office, legal department or other relevant supporting corporate services should be able to help with advice on export control issues. ECJU also provides a support point of contact which is able to advise on whether a particular end user is likely to be of concern or not. You can contact the ECJU on 020 7215 4594 or by email on eco.help@trade.gov.uk.

US Export Entity Control List: https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file

UN Sanctions List: www.un.org/securitycouncil/sanctions/information

Country Corruption Index: https://www.transparency.org/research/cpi

Trade Restrictions on Export: https://www.gov.uk/topic/business-enterprise/importing-exporting

ITAR (US International Traffic in Arms Regulations): https://www.gov.uk/guidance/exporting-military-goods-to-the-united- states#itar-uk-companies-and-dual-and-third-country-nationals

EAR (Export Administration Regulations): https://www.export.org.uk/page/UKUSExportControls

Compliance

ICO (GDPR/DPA): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-gdpr/

Intellectual Property Office (IPO) Lambert Toolkit: www.gov.uk/guidance/university-and-business-collaboration-agreements-lambert-toolkit

IPO: https://www.gov.uk/government/collections/ip-protection-abroad-country-guides

ATAS Academic Technology Approval Scheme: www.gov.uk/guidance/academic-technology-approval-scheme