Trusted Research & Innovation Attachment: Additional Information

Background
UKRI has a long-standing and ongoing commitment to effective international collaboration in research and innovation and is committed to ensuring that this continues to take place with integrity and within strong ethical frameworks considering potential risks where relevant.

UKRI has set out Trusted Research and Innovation (TRI) Principles, to outline its expectations of organisations funded by UKRI in relation to due diligence for international collaboration. Organisations funded by UKRI are expected to adopt these principles and be able to evidence the controls and measures that have been put in place that are consistent with these principles.

MRC TRI additional information guidance
This TRI document aims to provide applicants with additional space and guidance to provide details of any potential risks and associated mitigating controls related to international collaboration in light of the UKRI TRI programme, and the National Security and Investment Act (NSIA).

This information will be provided to the MRC's funding panel and will also inform an MRC TRI risk assessment if your proposal is successful.

All questions are based upon the UKRI TRI Principles, and we recommend referring to that document when completing this assessment.

The MRC is piloting this approach to gathering TRI information and there is no page limit in place whilst we carry out this pilot. Succinct answers are requested. As this is a pilot, future calls may have a different approach as we are continually seeking to improve and refine our processes.

Useful Links and Resources
Research Collaboration Advice Team (RCAT)
RCAT is a government and academia collaboration which provides research institutions with a first point of contact for official advice about national security risks linked to international research. RCAT works across government to make national security advice accessible and digestible for the academic community.

UK researchers can request advice on international research collaboration from RCAT. Within research institutions, communication with the RCAT should be conducted through your institution's nominated RCAT point of contact. If you are unsure who this is, please contact your Research Office. The Research Collaboration Advice Team covers the UK through regional representatives who continue to support specific institutions in their area.

Additional guidance and supporting information can be found from the following resources:
- UKRI TRI Webpages
- National Protective Security Agency (NPSA) "Trusted Research Guidance for Academia"
- Universities UK (UUK) Managing risks in Internationalisation: Security related issues
- Universities UK (UUK) Oversight of Security – Sensitive Research Material in UK
- Academic Technology Approval Scheme (ATAS)
- Export Controls Applying to Academic Research

TRI Attachment format, considerations and additional Information

The TRI attachment must be a PDF, using Arial 11pt typeface with margins of 2cms on all sides. To assist us with the assessment of your application, it is essential your TRI attachment is submitted separately to your application via email (ISPFattachments@mrc.ukri.org) by Wednesday 7th June. For more information, please see the Call Specific guidance.

In your TRI Attachment you should address the sections below.

Section 1: Due diligence of international partners

This section asks you to consider international connections that your project might have. This includes international connections through any of the UK organisations and individuals involved in the project. You should consider existing and potential financial and non-financial international collaborative partner organisations and/or individuals, bearing in mind:
- the collaborating individuals, partners and affiliations
- the nature of the activity and the envisaged outputs
- the potential for unethical or dual-use of information and/or outputs

It is recommended that you seek guidance from RCAT if you require external advice, but this is not a requirement. Please detail any external advice you have received.
When answering the questions below, you should consider whether your international collaborations could present any potential risks, outline any due diligence that has been completed and any reasonable and proportionate mitigations you will put in place.

1. Could any of the individuals associated with the project and/or their affiliations represent a conflict of interest that poses a potential risk in your view, for example, whether any military affiliations, other employment/sources of income, or upheld allegations of breaches of research integrity or ethical standards? If yes, what mitigations will be put in place?

2. Could a partner organisation or their affiliations pose a potential risk in your view related to their legal framework and constitution and/or the country in which they are based and the laws that govern how they operate? If yes, what controls will be put in place to reduce risk?

Section 2: managing information and knowledge sharing

This section asks you to consider the data your study will be collecting and producing, as well as how this data will be managed by the research team, with a particular focus on how sensitive data is shared with, and accessed by, the overseas collaborators. Your approaches should comply with UK legal requirements, including the Data Protection Act 2018.

Please focus here on the <u>international security aspects</u> to avoid duplication with the Data Management Plan.

3. Describe your information security management and strategy considering:
   i. Establishment and maintenance of a robust cyber-security culture
   ii. Identification and storage of sensitive data and information
   iii. Access management for sensitive data and information

    iv.   Potential for data and information misuse (including risks of dual use) and other unethical application of project data outputs

4. UK and overseas legislation

Have you considered the impact of relevant legislation of overseas partners? Does any overseas legislation permit authorities to access sensitive information without consent from all parties?

5. Risk reduction

Could any of the proposed research activities pose potential information and knowledge sharing risks? If yes, what controls will be put in place to reduce risk?

Section 3: managing research outputs and intellectual assets

Collaboration agreements should be put in place between all partners to ensure that sensitive data and any intellectual assets, including intellectual property rights, derived from the project are appropriately managed to enable future commercial outcomes to be realised which could lead to societal and economic benefit.

This section asks you to consider potential outputs which could be relevant from a commercial perspective, and how the associated assets would be managed in light of trusted research considerations.

6. Intellectual Assets and Intellectual Property (IP) Rights
Have you considered how any intellectual assets (for example data, results, methods) including any IP arising from the project will be managed? This might include proposed IP ownership and consideration of when it is most appropriate to seek protection for any intellectual property and subsequently how to exploit or disseminate it to maximise its impact. This should not conflict with other UKRI requirements, for example open access policy.

7. Publishing project outputs
Have you considered your approach to publications, particularly when this might involve commercially relevant and/or commercially sensitive data and/or findings derived from the project? How would you decide whether any protection for the intellectual assets should be sought prior to publication? When a decision is made to publish research findings, the outputs should comply with UKRI's open access and open data policies and guidance.

8. Export controls
Have you considered whether UK export controls are relevant. All organisations funded by UKRI should ensure they understand export controls that may apply to their project and activities, from the export of materials to presentations at conferences.

9. Could any of the proposed activities pose a potential TRI/National security risk in your view regarding how intellectual assets could be commercially exploited or applied? If yes, what mitigations will be put in place?

Any other comments Please use this section to provide any further information or comments you think could be relevant but that did not align with the questions above.