# Research Security Review Criteria

The following serves as a resource for considering risks in international engagements. The term "engagement" can cover many different activities involving international parties, including the following examples: research collaborations, agreements, financial or in-kind support, services, intellectual property licensing, investments, physical exports, material or data transfers, or others.

The document is broken into four sections by type of review. Each section has a list of criteria that should be considered when conducting research security reviews or risk assessments.

The review criteria is intended to serve as a list of possible considerations. Not all criteria may apply to every situation. Depending on the engagement, decide which criteria applies and who should review.

It is recommended that you document your reviews, including who is responsible, the process followed, results of the review, and decision made about the engagement.

Records should be kept in accordance with the relevant policy and regulatory requirements.

## TABLE OF CONTENTS



## General Review

1. Conduct *"Know Your Customer"* due diligence for research security risks. *"Know your customer"* is a concept used by the Department of Commerce under the Export Administration Regulations (EAR)[1] to communicate the need to conduct a reasonable level of due diligence or vetting on foreign parties before transacting with them. Since export controls concentrate on the nexus between international parties and emerging technology, many export control concepts, such as "know your customer," can be utilized for research security reviews, where broader reputational, regulatory, legal and financial risks are considered. U.S. lawmakers want universities to consider risks related to the development of foreign military capability, US economic competitiveness, and human rights concerns.

   "Know your customer" is crucial for export control compliance. In performing a research security review, it can also be adapted for academic purposes as "know your collaborator." As part of "*know your customer"* you must complete due diligence reviews.

   Due diligence includes screening against government and other lists (see the BIS Compendium of Resources), identifying what value is transferred to the foreign party, and

[1] Supplement No. 3 to Part 732 of the Export Administration Regulations

establishing the ultimate purpose (or end use) of the transferred items or information. Certain end uses, such as weapons proliferation, are prohibited.

Examples of due diligence reviews that should be conducted on partners in countries of concern include:

- ☐ Restricted Party Screening for entities and key individuals (including research collaborators) as identified by the location's research security reviewer.
- ☐ Review publicly available or other sources of information for:
  - ties to a foreign government or military
  - evidence of military research and development
  - evidence of foreign talents program participation
  - organizational connections or relationships with other restricted, government or military entities

2. Consider the engagement in context, by identifying peripheral agreements that are related to the engagement, such as non-disclosure or material transfer agreements. Those peripheral agreements should be reviewed by the location in relation to the primary engagement.
3. Conduct a risk analysis considering the following factors, among others[2].
   - ☐ Is there a significant risk that the discoveries and inventions arising from the project could be used against the national security interests of the United States? Does the engagement involve research that the United States government has proposed to impose restrictions on or restricted in part or in whole, e.g., semiconductors and supercomputers?
   - ☐ Will the engagement benefit a foreign government or foreign corporations in a way that would negatively affect the competitiveness of the U.S. economy?
   - ☐ Will the collaborating organization benefit from the unpublished know-how that UC researchers have developed during previous U.S.-government-funded research?
   - ☐ Will the collaborating organization benefit from access to UC equipment or facilities that have been funded by the U.S. government?
   - ☐ Will the engagement involve any of the research security risks set forth in Department of Defense's June 29, 2023 Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education? In particular, does the engagement run the risk of constituting a "malign foreign talent recruitment program" as defined in Section 10638(4) of the CHIPS and Science Act of 2022 (Public Law 117-167)?
   - ☐ Does the engagement involve an advisory board whose foreign industry participants financially sponsor research, receive access to pre-publication research and/or obtain intellectual property rights to research? What are the affiliations of other board members or charter of the board—are there any red flags?
   - ☐ Is the engagement clearly articulated?

[2] Additional considerations are outlined in the following:
See page 37, 7.3 Assessment Tools - National Science Foundation commissioned JASON report. NSF commissioned this academic think tank to consider the issues around foreign influence and best practices to address it.
See page 44, 7.5 Review Category 5: Extramural Funding Opportunities - NIST: Safeguarding International Science: Research Security Framework.

- ☐ Are there foreign talent recruitment program participants?
- ☐ Are there military end users or military intelligence users involved?
- ☐ Are there military or military intelligence end uses of the technology?
- ☐ Does the foreign collaborating entity, foreign collaborator, or other engagement participant have a close tie to the foreign government's defense sector? Is there foreign government funding involved? Is a foreign government involved in governance and/or management related to the project or approving research or operations funding?
- ☐ If the engagement involves shared governance, management, financial risk, or operations, is the location receiving the information it needs to exercise oversight and ensure the location's legal compliance?
- ☐ If the engagement involves visitors from participating organizations, are there safeguards that should be considered with respect to the visitors' activities, such as documented safeguards to ensure non-access to or non-participation in sensitive federal research?
- ☐ Are there affiliations with restricted entities or other entities of concern, including but not limited to entities accused of human rights violations, entities that were previously restricted and/or entities criminally charged by the United States government?
- ☐ Does the engagement include use of the UC name and are planned activities consistent with the relevant policies that govern such use?
- ☐ Is the engagement collaborative in nature or does it appear to exclusively involve funding or support by the collaborating organization in exchange for teaching, mentoring and/or research by the location?
- ☐ If the engagement involves the licensing of any intellectual property, is the license consistent with UC policy? Is the ownership of the IP appropriately protected? Does the licensing arrangement disproportionately favor the collaborating organization?
- ☐ If required, has the location ensured the engagement is included in foreign source gift or contract reports under Section 117 of the Higher Education Act?
- ☐ What are the reputational risks to UC? Are you aware of any adverse media reports? Have you consulted External Relations (Communications), Federal or State Government Relations, General Counsel, or other relevant offices to consider reputational risks?
- ☐ If the engagement involves legal or other risk, have compliance and/or due diligence mechanisms been considered?
- ☐ For any large-scale activity in which media or website coverage is planned, is there a policy or protocol by which any such media or website announcements are reviewed by the location's legal or compliance staff?
- ☐ Are there mechanisms to ensure updated and/or periodic reviews of these and the other risks noted in this review criteria or are such reviews triggered by substantive changes in the engagement?

## Export Control Review

Export license reviews take into consideration many factors, including item, technology, parties to the transaction, destination, end use and end user. The location Export Control Officer is *"responsible for reviewing the applicability of export control regulations and/or determining options for export licensing, exceptions, or control plans to mitigate risk*[3]*."* See UC Export Control Policy for federal regulations and more details on roles and responsibilities.

- ☐ Perform a license review to determine legal requirements, which include tangible and intangible items.
- ☐ Perform an end use and end user review.
- ☐ Perform "*Know your customer*" due diligence for export license requirements. *"Know your customer"* is a concept used by the Department of Commerce under the Export Administration Regulations (EAR)[4] to communicate the need to conduct a reasonable level of due diligence or vetting on foreign parties before transacting with them.
- ☐ Perform a "General Prohibition" review, paying close attention to potential financial or services transactions with foreign parties subject to export controls where you have "knowledge" that a violation may occur (i.e., GP 10), using the due diligence best practices outlined in guidance issued by BIS on October 9, 2024.
- ☐ Consider enhanced and customized export control training.
- ☐ Consider requiring the researcher to execute a written research management plan describing the planned activities, the required export control safeguards, and periodic updates of such a plan.
- ☐ Consider research security measures if research is intended to be shared with a foreign partner to ensure that export controlled information is not shared, e.g., written questionnaires and/or use of a pre-publication databank.
- ☐ Consider requiring a description of any planned use of restricted technology and the notification and approval of the export control officer prior to purchasing or exporting any restricted technology.
- ☐ Consider requiring a description of any planned mentoring of foreign individuals and notification and approval of the export control officer prior to any change in mentoring plans.
- ☐ Consider requiring a description of any planned lab tours and notification and approval of the export control officer prior to the performance of such tours.
- ☐ Consider for any large-scale engagement whether appointment of a dedicated export control compliance resource is warranted.

[3] UC Export Control Policy https://policy.ucop.edu/doc/2000676/ExportControl
[4] Supplement No. 3 to Part 732 of the Export Administration Regulations

## Disclosure Review

Federal funding agencies have identified transparency as fundamental to the integrity of research and funding decisions. Under UC policy and federal funding agencies, UC has an institutional obligation to accurately disclose potential conflicts of interest and commitments to federal funding agencies and to maintain institutional oversight of the federal awards granted to UC.

1. Gather internal information to identify and address non-disclosure risks.
    - ☐ Identify federal funding for the researchers involved. Note that each federal funding agency may have specific and unique requirements.
    - ☐ Implement a continuous process to identify and address disclosure gaps. The process may involve requesting additional information from participants.
2. Provide detailed disclosure guidance and training to participating researchers based on their federal funding, federal sponsor requirements, and the information gathered in this process.
3. Consider the following for large-scale engagement:
    - ☐ Drafting and circulating a template(s) for federal disclosures for researchers and research administrators.
    - ☐ Informing the research administrative unit assisting researchers on their proposals of the collaboration and the need to disclose it in federal proposals.
    - ☐ Identifying when more extensive and/or one-on-one disclosure training should be provided.
    - ☐ Briefing researchers on how to accurately and/or specifically list affiliations with foreign entities and/or acknowledgments of foreign funding in publications.
    - ☐ Including guidance for publications that cite both federal and foreign support, detailing how to differentiate the portions of the publication supported by federal support versus foreign support.
4. Consider holding town halls and providing written guidance on specific disclosure issues for researchers including whether:
    - ☐ Compensation for non-research tasks may be disclosable to federal agencies as support and,
    - ☐ Classifying different kinds of in-kind support (e.g., staff, including visiting individuals, equipment and supplies) and how to disclose this support to federal funding agencies.
5. Determine a process for researcher disclosure support, pre-proposal review, and ongoing monitoring of researcher disclosures.

## Legal Review

The decision to proceed with a high-risk engagement is complex because it can potentially carry significant reputational, regulatory, legal, and financial risks. If not managed successfully, these engagements can result in loss of federal research funding opportunities, reputational damage, or potential export violations, which could result in civil or criminal penalties. Conduct a review that considers the following:

- ☐ Identify regulatory risks and liabilities.
- ☐ Determine financial risks.
- ☐ Identify reputational risks.
- ☐ Determine whether a mitigation plan exists to address the known risks.