UC International Engagement Enhanced Review and Approval Guidance

The following guidance for the Enhanced Review and Approval Process described in President Drake's letter consists of Frequently Asked Questions (FAQs), Definitions, and Research Security Review Criteria.

TABLE OF CONTENTS

FREQUENTLY ASKED QUESTIONS

1. Why has the President decided to issue this new review and approval requirement?

On August 28, 2023, the President issued a letter to the Chancellors and Lawrence Berkeley National Laboratory Director outlining a new comprehensive framework (herein referred to as "framework") with three core requirements for any University of California (UC) international affiliations and agreements involving emerging technology and countries of concern. These new requirements are intended to proactively protect our intellectual property, strengthen our collaborations, and preserve the reputation of our research enterprise.

As the largest public university system in the world, the University of California cannot achieve its mission of education, scientific advancement, and public service without global engagement and an international perspective. UC also benefits immensely from international collaboration and engagement with the global scientific community.

Simultaneously, UC has a responsibility to recognize that the inherent risks involved with international engagements have changed. Emergent risks include undue foreign government influence, participation in activities or with partners counter to UC's values, and undefined or asymmetrical expectations in international partnerships.

Federal agencies leading research sponsorship, like the National Science Foundation (NSF) and the National Institutes of Health (NIH), as well as other universities and academic associations like the National Academies of Sciences, have all recognized these emergent risks and issued recommendations on how to consider the risks thoughtfully to successfully navigate them without disengaging from international cooperation and partnerships.

UC must align with these recommendations and any relevant federal requirements for sponsored research awards while continuing to strengthen our mission and uphold our values. The new framework serves to advance these goals for the system.

2. Where is this new requirement on international engagements coming from?

The federal government is concerned about undue foreign influence from a handful of countries and their governments that systemically target universities and our open environment to gain technological or strategic advantage.

The federal government has issued new communications, guidance, and requirements to address their concerns related to certain countries and emerging technologies (see FAQ 8 and 9 below). Concerns include U.S. national security and foreign policy, as well as efforts to maintain strategic and economic advantages in specific areas and the need to prevent further human rights abuses by some regimes.

In addition, the UC policy on International Activities requires international activities comply with "all applicable state and federal laws and regulations, UC policies, and the laws and regulations of foreign sites." The policy also requires proponents of international activities to consider potential risks and create a plan to mitigate and/or minimize identified risks. International activities should also align with UC ethics and values, along with the faculty code of conduct.

This Policy applies to all international activities at UC and clarifies which activities must be approved by the Regents, the President, or the UC Provost, with the President reserving "the authority to approve very high-risk matters."

3. Can you provide definitions for the terminology used in the letter, such as engagements, agreements, affiliations, or collaborations?

Yes. Definitions are provided at the end of this FAQ.

4. What international activities require "Enhanced Review and Approval" by UCOP?

International affiliations and agreements[1] involving emerging technology[2] and countries of concern[3] require Enhanced Review and Approval by UCOP.

In this guidance, the term "Engagements" serves as a "catch-all" term to encompass international engagements, affiliations, agreements, and collaborations (see Definitions).

Locations should begin by determining whether the activity meets the definition of an international Engagement, followed by whether the Engagement involves BOTH a country of concern AND an emerging technology.

If both of those criteria are met, locations should assess whether the Engagement is at the "Institutional Level" (see Definitions). Engagements at an Institutional Level that involve BOTH a country of concern AND emerging technology are considered "In Scope" and therefore require Enhanced Review and Approval.

When assessing whether emerging technology is involved as part of the Engagement, you cannot limit knowledge to what is written in an agreement or proposal. For example, if an MOU or student exchange agreement does not specifically call out artificial intelligence, but the lead researcher's field or the students' field of study is AI, the location should ask clarifying questions around what is involved in the Engagement. See answers 13, 14 and 15 as well as the UC International Engagement Research Security Review Criteria (herein referred to as "Review Criteria") later in this guidance for ideas on what questions to ask depending on the Engagement.

---

[1] "UC international affiliations and agreements" encompass "Engagements, affiliations, and agreements including but not limited to sponsored research agreements, proposals, gifts, international agreements, degree granting programs, and memoranda of understanding."

[2] For the purposes of the new framework, emerging technologies include those listed by the Department of Commerce, Bureau of Industry and Security in 83 FR 58201, including but not limited to Artificial Intelligence (AI) and Machine Learning, Quantum Information/Sensing, Semiconductor and Microelectronics, Biotechnology, and other areas that can be identified by your Export Control Officer (ECO) based on evolving federal government classification of emerging technology important to national security. See question 9 for more detail.

[3] For the purposes of the new framework, "Countries of concern" include Qatar, Saudi Arabia, United Arab Emirates, the People's Republic of China (including Hong Kong and Macau), the Democratic People's Republic of Korea (North Korea), the Russian Federation, and the Islamic Republic of Iran. See e.g., Section 19221 of the CHIPS and Science Act of 2022 [42 U.S. Code § 19221]; Section 117 of the U.S Higher Education Act of 1965; and https://www2.ed.gov/policy/highered/leg/institutional-compliance-section-117.pdf." See question 8 for more detail.

Engagements that are assessed to be Out of Scope still need location research security reviews to identify and mitigate any relevant legal, compliance, financial, or reputational risks.

In addition to Individual Level Engagements, here is a short list of Institutional Level activities that would be Out of Scope even if they involve countries of concern and emerging technologies:

OUT OF SCOPE INSTITUTIONAL LEVEL ACTIVITIES

Agreement type	Purpose	What may be exchanged
Non-disclosure Agreement (NDA) or Confidentiality Agreement (CDA)	Transfer of information	Proprietary or confidential information
Federally Sponsored grants or contracts, federally sponsored research with foreign subawards, or federally sponsored research with foreign-located collaborators	Financial support for research from a federal agency	Technology, items, software
Sales and Service Agreement	Sale of a UC service related to location facilities, operations, or procurement	Technology, items software
Material Transfer Agreement (MTA)	Material transfer	Technology, items, software
Data Use or Software License Agreement (DUA/SLA)	Transfer of information or software	Technology, information, software
Patent/Intellectual Property licensing[4]	Further technology development	Rights
Purchasing or procurement	Operational purchase of supplies, equipment and services	Goods and services
Gifts *under* $50,000 from a foreign source associated with a country of concern	Provides funding for research, capital projects, or other purposes	Goods and services
Degree granting programs without a research component or exchange	Agreements for educational exchanges between institutions	Educational services

[4] For patent/IP licensing, the location IP licensing/tech transfer office should coordinate with the local ECO for export license reviews and other stakeholders to conduct research security reviews.

In contrast to Institutional Level, Individual Level Engagements, like faculty appointments, affiliations, presentations, or collaborations where there is no ongoing Institutional Level Engagement or commitment, do NOT require Enhanced Review and Approval. Examples of Individual Level Engagements include:

- Individual visiting scholars or students (student or other exchange agreements are In Scope).
- Individual faculty collaborations and Engagements, e.g., a speaking engagement.
- Outside Professional Activities undertaken by faculty in their individual capacities. [5]

Gifts of $50,000 or more from a foreign source associated with a country of concern that involves emerging technology are In Scope for Enhanced Review and Approval, while gifts that do not meet that threshold are Out of Scope. The $50,000 threshold aligns with Sec 10339B of the CHIPS and Science Act of 2022. See FAQ 8 for the list of countries of concern.

Degree-granting programs with research or exchanges are considered as In Scope Engagements, while purely degree-granting programs are Out of Scope.

Any other Engagement that involves both a country of concern and an emerging technology NOT identified in the above table and that is undertaken at the Institutional Level should be considered In Scope and sent to UCOP for review and approval. A location can write to researchsecurity@ucop.edu to request clarification.

5. How do locations submit requests for approval to the Office of the President?

Each location should develop a process for ensuring that the following steps are taken to secure Presidential approval for any location international Engagements (including affiliations, and agreements):

1. Review the FAQs and Review Criteria in this guidance. Any relevant compliance, legal, and research security review items from the Review Criteria must be addressed through local review prior to sending items to the Office of the President.
2. The responsible party designated by the location leadership should consult with relevant location expertise (e.g., export control review performed by the Export Control Officer, Campus Counsel, Research Compliance), compile input, and consult with location leadership about whether to proceed with an Engagement. Once relevant location approvals and consultations are completed and a location decision is made to proceed with an Engagement, move to step three below.
3. Complete the UC International Engagement Submission Form (herein referred to as “Submission Form”) provided by UCOP detailing the proposed Engagement, including the consultation and review process (legal, compliance, etc.), and risks (legal, financial, or reputational) identified through local review. Outline relevant mitigation steps that have been or will be taken to address any risks.

[5] Outside Professional Activities undertaken by faculty are governed by Academic Personnel Manual Sections 025 and 671.

4. Named location officials must sign the Submission Form confirming that location-identified concerns have been resolved or mitigated such that they recommend proceeding with the proposed Engagement. A location official must also sign the Submission Form, acknowledging that the Chancellor was briefed on the Engagement and that any location concerns have been resolved or mitigated.
5. The completed and fully signed Submission Form must be emailed to researchsecurity@ucop.edu.
6. ECAS, in consultation with RPAC and UC Legal, will review the Submission Form. We may contact you with additional questions if the form does not appear complete.
7. Completed forms will be forwarded to the President's Executive Office for President Drake's review and approval.

6. What should be included in the location review?

Use the Research Security Review Criteria as part of the location review.

7. How can locations ensure that researchers or other parties to the proposed international Engagement with countries of concern and emerging technology understand the legal, regulatory, and policy implications?

Locations should provide training tailored to the specifics of the Engagement and deliver it to researchers and administrators involved in the proposed Engagement. The training should aim to raise awareness of all relevant federal or state laws and regulations, along with UC policies. For example, researchers involved should receive training to ensure accurate disclosures in federal grant proposals and enhance their understanding of any export control regulations pertaining to the Engagement.

8. What is a Country of Concern?

For the purposes of the framework, countries of concern include China, Iran, North Korea, Russia, Qatar, Saudi Arabia, and the United Arab Emirates. International Engagements involving these countries represent higher risks for institutions of higher education based on federal regulations and policies in these two areas:

1. The Sec 19221 of the CHIPS and Science Act of 2022 identifies China, Iran, North Korea, and Russia as countries of concern for reasons of national security.
2. The Department of Education's report on Institutional Compliance with Sec 117 of the Higher Education Act of 1965 identified China, Qatar, Saudi Arabia, and the United Arab Emirates as the top foreign sources of funding to U.S. institutions of higher education by total amount (more than $1 billion of the total $6.6 billion reported in 2020). According to this report, funding from China, Qatar and Saudi Arabia came largely from the instrumentalities of those countries' governments, which may carry a higher risk. The University of California is committed to HEA Sec 117 compliance, and therefore contributions originating from or Engagements with these countries should undergo thorough review.

Due to the possibility of further federal government actions, consider this list dynamic and subject to future updates by UCOP.

9. What is Emerging Technology?

As a term, Emerging Technology can be used broadly to mean different specific technology areas for various purposes. For the purposes of reviewing international Engagements and affiliations in relation to the President's Letter, Emerging Technology means a specific but evolving list of technology areas under Sec 1758 of the Export Control Reform Act (ECRA). Research on and with these technologies, which include Engagements with countries of concern, needs to be reviewed by the location first and then routed for Enhanced Review and Approval. Based on various federal guidance[6], technology areas considered Emerging Technology include:

- Biotechnology (Note: currently, the government has identified the following areas of biotechnology as emerging technology: Nanobiology, Synthetic biology, Genomic and genetic engineering, Neurotech).
- Artificial intelligence (AI) and machine learning
- Positioning and navigational technology
- Microelectronics or Semiconductors
- Advanced computing
- Data analytics technology
- Quantum information and sensing
- Additive manufacturing
- Robotics and autonomous systems
- Brain-computer interfaces
- Hypersonics
- Advanced materials
- Advanced surveillance

UCOP will update this list periodically, but it is recommended that locations consult the Export Control Officer regularly for the most current information on how the federal government is looking at Emerging Technology.

10. Are individuals who are nationals from countries of concern working or studying on our locations considered In Scope?

No. A foreign national visiting as a scholar or a student should be vetted through local processes developed in response to the systemwide Foreign Influence Audit and based on guidance UCOP published in January 2022. Locations should follow their vetting process, including escalating high-risk Engagements to leadership.

In addition, individual visiting scholars and students, other visitors, or visiting delegations outside of an Institutional agreement do not need to be submitted.

[6] Export Control Reform Act (ECRA) draft; White House Office of Science and Technology Policy (OSTP) Critical and Emerging Technologies List Update from 2022; and the Center for Strategic International Studies (CSIS) report on Optimizing Export Controls for Critical and Emerging Technologies. Note: the federal government is regularly updating and refining what they consider to be Emerging Technology.

However, if there is an overarching Institutional agreement, such as an MOU or exchange agreement in place with a country of concern and that agreement involves emerging technology it requires Presidential review and approval, and should be included in the submission process to UCOP.

11. What is the timing for Enhanced Review and Approval?

A complete submission containing enough information for a thorough review by ECAS, RPAC, and UC Legal can be reviewed completely between ECAS, RPAC and UC Legal, minimizing review time. If a submission is incomplete, the submission will be returned to the location with a request for additional information, increasing the response time.

12. Proposal submissions often have hard deadlines. How will UCOP handle these very time-sensitive items?

When a proposal is identified as subject to the criteria for Enhanced Review and Approval, all parties to the proposal should be notified that it requires Presidential approval prior to submission. A best practice is to identify these types of Engagements with countries of concern in emerging technologies early in the proposal process so that there is sufficient time for UCOP review and Presidential approval. If a proposal is submitted to a funding entity prior to review and approval by the President, the sponsor and proposer (i.e., principal investigator or responsible party) should be notified that approval by the President must be secured before the location can accept a subsequent agreement or support.

13. Can you provide additional resources for locations to utilize in their reviews?

UCOP recommends that locations review and utilize relevant guidance and information provided by the federal government in their efforts to conduct research security reviews.

- Research Security at the National Science Foundation. NSF has taken the lead in developing research security practices for federal agencies that sponsor research. NSF created a webspace dedicated to communicating requirements, guidance, and expectations.
- Foreign Interference, the National Institutes of Health. NIH created this website dedicated to foreign interference (i.e., influence), where the agency shares news, guidance and requirements to better educate the extramural research community on these issues.
- Department of Commerce, Export Administration Regulations, Supplement 3 to Part 732, "Know Your Customer." The Department of Commerce uses this concept as a foundational tenet of an export control program. Beyond export controls, the concept also has utility for conducting research security or other types of international Engagement reviews performed at the location. "Know Your Customer" is discussed in more detail in the Review Criteria.
- Academic Research Security, Department of Defense. Like NSF and NIH, DoD has created its own resource website with guidance and resources on research security, as well as new requirements that DoD is implementing related to research security. DoD takes a risk-based approach and does not allow researchers to participate in malign foreign talent recruitment programs. Review any DoD-sponsored research.

- The National Science and Technology Council Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise. This document is meant as a supplement to the NSPM-33 guidance for universities to use during research security reviews.
- The National Science Foundation commissioned JASON report See page 37, 7.3 Assessment Tools. NSF commissioned this academic think tank to consider the issues around foreign influence and best practices to address them.
- NIST: Safeguarding International Science: Research Security Framework See page 44, 7.5 Review Category 5: Extramural Funding Opportunities.

14. What UC resources can we utilize?

These guidance documents include discussions on roles and responsibilities and export control risks that will be useful for all stakeholders in the international Engagement review process.

- ☐ Export Control Red Flags Guidance
- ☐ Restricted Party Screening Roles and Responsibilities
- ☐ International Scholar Vetting

Research security video shorts:
https://www.ucop.edu/ethics-compliance-audit-services/compliance/export-control/research-security-video-shorts.html

In addition, ECAS has created a Research Security Resources webpage with these resources and will add new resources as they become available.

15. What are some general information sources we can use to perform research security reviews?

- Public search of available sources, including court filings and U.S. government announcements.
- World-Check One: a subscription database providing business intelligence data.
- Lexis Nexis: subscription legal document repository.
- Visual Compliance: subscription software that facilitates screening against restricted parties and entities of concern lists.
- Consolidated Screening List: https://2016.export.gov/ecr/eg_main_023148.asp

16. What kind of records should be kept?

Locations should keep records related to all reviews and at minimum, document reviews and retain that documentation as required by any applicable regulation or policy. For example, Export Control record-keeping requirements are a minimum of five years under the regulations. These requirements are also outlined in the UC Records Retention Schedule and in the UC Export Control policy.

17. Once approved by UCOP, are there any follow-up steps locations need to take once the international Engagement begins?

Yes, the location should have a process for monitoring Engagements to account for potential material changes, new regulatory rules, or enforcement priorities, or other changes that might occur as the Engagement progresses.

Recognizing that arrangements can and do change over time, if the information originally submitted to UCOP for approval needs to be updated in the future, please send a message to researchsecurity@ucop.edu.

18. The Engagement, affiliation, or agreement I'm reviewing isn't covered here or I have additional questions. What should I do?

Any international Engagement (including any affiliation or agreement) not specifically cited in this FAQ as Out of Scope should be considered In Scope and require Enhanced Review and Approval if it involves both a country of concern and an emerging technology. If you have questions or want specific clarification on whether Enhanced Review and Approval are needed, write to researchsecurity@ucop.edu.

DEFINITIONS

Agreements: A manifestation of mutual assent by two or more parties, made through offer and acceptance. An agreement can be written or oral. Forms of agreements may include contracts, gift agreements, corporate sponsorship agreements, grant agreements, and memoranda of understanding.

Engagements: A general term used to describe an activity that the University or any of its components undertake at the Institutional Level that involves significant or meaningful interaction or exchange with another entity. For the purposes of the President's letter, "Engagements" is a "catch-all" term to describe Agreements, Affiliations and Collaborations that need to be considered and sent to the President for review and approval if they involve a country of concern and emerging technologies.

Affiliation: An association or relationship of a continuing nature between the University or any of its components (e.g., location or location sub-units) and another organization or individual in support of an academic, research, clinical and/or scholarship program and/or exchange of students, faculty, scholars, and staff.

Collaborations: A general term used to describe an activity that the University or any of its components undertake at the Institutional Level that involves significant or meaningful interaction or exchange with another entity. For the purposes of the President's letter, this term is used interchangeably with "Engagements."

Institutional vs. Individual Levels: For the purposes of the President's letter, international Engagements that are undertaken by or on behalf of the University, a location or any of its components are considered at the "Institutional Level." In contrast, agreements that are NOT undertaken by or on behalf of the University, a location or any of its components are considered

to be undertaken at the “Individual Level.” Examples of Individual Level affiliations and agreements include professional relationships between a researcher acting in their individual capacity and international parties to collaborate on a research project or co-author a scientific journal.

In/Out of Scope: Engagements that are “In Scope” mean they DO require Enhanced Review and Approval, while Engagements that are Out of Scope do NOT require Enhanced Review and Approval. Engagements or activities that involve countries of concern and emerging technology should be assessed by the location to determine whether they are In or Out of Scope for the Enhanced Review and Approval requirement outlined in item 1 of the President’s letters. **Importantly, Engagements that are assessed to be Out of Scope still need location research security reviews to identify and mitigate relevant risks**.

Enhanced Review and Approval: For the purposes of these guidance documents, when the phrase “Enhanced Review and Approval” is used, it means specifically pursuant to President Drake’s Letter to the Chancellors and LBNL Director on August 28, 2023, and does not mean to be comprehensive of other policies or processes, such as the International Activities Policy, where Enhanced Review and Approval may be required separate of the President’s letter.

RESEARCH SECURITY REVIEW CRITERIA

Below is a list of criteria that must be reviewed and considered by the location prior to completing a Submission Form to request Enhanced Review and Approval from UCOP. The Review Criteria have been organized into four areas plus an appendix:

The location is responsible for deciding how each review will be completed. Some options include assigning the review to an official with the relevant knowledge, experience, and duties; convening a committee or other group to share the review responsibilities; or creating a process that completes all the Review Criteria through various processes and areas of responsibility.

The Review Criteria is intended to serve as a list of possible considerations. Each criteria must be considered when reviewing your Engagement.

The location must document how the review was conducted, who is responsible for confirming review completion, and then document the review, result, and decision. Records should be kept in accordance with the relevant UC policy or regulatory requirements.

Review information and results should be provided to the officials signing off on the Submission Form and briefed to the Chancellor.

The Review Criteria can also be used at the location as guidance or best practices for completing their own research security reviews on Engagements that are not In Scope for Enhanced Review and Approval.

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)[7] 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 question 15 of the UC International Engagement Guidance FAQs), identifying what value is transferred to the foreign party, and 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. Although some peripheral Agreements, such as non-disclosure agreements and material transfer agreements, do not require submission and approval under the Enhanced Review and Approval framework, those peripheral agreements must be reviewed by the location in relation to this Engagement. See the Appendix for examples.
3. Conduct a risk analysis considering the following, among other factors[8].

   - ☐ 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

[7] Supplement No. 3 to Part 732 of the Export Administration Regulations
[8] 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.

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 industrial advisory board whose foreign industry participants financially sponsor research, receive access to pre-publication research and/or obtain intellectual property rights to research?
- ☐ Is the Engagement clearly articulated?
- ☐ Are there foreign talent recruitment program participants?
- ☐ Are there military or military intelligence end uses of the technology?
- ☐ Are there military end users or military intelligence users involved?
- ☐ 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?

- ☐ 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*[9]*."* 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)[10] to communicate the need to conduct a reasonable level of due diligence or vetting on foreign parties before transacting with them.
- ☐ 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.

[9] UC Export Control Policy https://policy.ucop.edu/doc/2000676/ExportControl
[10] 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.

APPENDIX

Adapted from December 2021 "*Export Control Red Flags*" guidance document, which identifies university agreements and red flags. To consider the Engagement in context, identify peripheral Agreements that are related to the Engagement. Although some peripheral Agreements, such as non-disclosure agreements and material transfer agreements, do not require submission and approval under the Enhanced Review and Approval framework, those peripheral agreements must be reviewed by the location in relation to this Engagement.

This chart identifies Agreements that may be peripheral. For each agreement type, the purpose and transfers columns describe what the agreement might cover. Associated examples are also included, while red flags outline the risks. "*Red flags*" is a concept used by the Department of Commerce, to identify transactions that should be reviewed further. These "red flags", which are discussed in detail in the "Export Control Red Flags" guidance document, include both export control and research security risk factors.

Agreement type	Purpose	Transfers	Examples	Red flags
Non-disclosure Agreement (NDA) or Confidentiality Agreement (CDA)	Transfer of information	Technology (information)	Process Design Kits, "know how," intellectual property, designs, manuals, blueprints for sensitive items	Country of Concern or foreign military related sponsor, agreement language limits publication, participation or intellectual property rights, involves controlled technologies, involves restricted parties or entities of concern
Research Agreement	Financial support for research	Technology, items, software	Funds, know how, intellectual property, materials, equipment	Country of Concern or foreign military related sponsor, agreement language limits publication, participation or intellectual property rights, involves controlled technologies, involves restricted parties or entities of concern
Memorandum of Understanding or Research Collaboration Agreements	Institutional agreements establishing partnerships or other unfunded activities	Technology, items, software, information	MOU, research collaboration or other agreements that agree to exchanges of information, students, personnel or material	Country of Concern or foreign military related partner, involves controlled technologies, involves restricted parties or entities of concern
Sales and Service Agreement	Sale of a UC service	Technology, items, software	Projects under Sales and Service are not research and therefore subject to export controls (i.e., they do not qualify under the umbrella of the Fundamental Research Exclusion), there may be high risk for receipt of controlled information, items or software or development of those	Country of Concern or foreign military related sponsor, agreement language that varies from UC standard language, collaborations that involve controlled technologies, involves restricted parties or entities of concern

Agreement type	Purpose	Transfers	Examples	Red flags
International Agreement	Exchange agreements	Technology, items, software	Agreements with foreign universities, companies or scholars to arrange exchange visits or to engage in collaborative research or activities may involve engagements with restricted parties, military end users, or entities of concern	Country of Concern or foreign military related sponsor, agreement language limits publication, participation or intellectual property rights, involves controlled technologies, involves restricted parties or entities of concern
Material Transfer Agreement (MTA)	Material transfer	Technology, items, software	Material Transfer Agreements or other IP transfer where tangible items and international shipments are involved	Physical exports, Country of Concern or foreign military related sponsor, agreement language limits publication or intellectual property rights, involves controlled technologies, involves restricted parties or entities of concern
Data Use Agreement (DUA) or Software License Agreement (SLA)	Agreement to receive licensed software or proprietary data	Technology, software	Data use agreements, software license agreements and other agreements signed on behalf of the institution may be for sensitive information or software or may contain language indicating an export control issue	Country of Concern or foreign military related sponsor, agreement language limits publication, participation or intellectual property rights, involves sensitive data or emerging technologies, involves restricted parties or entities of concern
University Extension or other Education Services Agreements	Agreement or activity to provide non-catalog course education to non-matriculated students	Technology	Non-catalog courses may not qualify for the general education carve outs under export control regulations. Providing education to students in a sanctioned country, associated with a restricted party, or who are nationals of a sanctioned country may require an export license. Additionally, agreements or activities with institutions or organizations in a sanctioned country or on a restricted party list may also require an export license.	Country of Concern or foreign military related sponsor, involves controlled technologies, involves restricted parties or entities of concern