GUIDANCE DOCUMENT DECEMBER 2021

EXPORT CONTROL RED FLAGS GUIDANCE

KEY TAKEAWAY

Sponsored research or other agreements with outside partners often involve university activities with elevated export control risks, such as international shipments, international collaborations or work with export controlled technology. The agreement language or statement of work offer the first opportunity to identify these risks and address them before a potential violation. This guidance document serves to describe the potential risks, presented as "red flags," and best practices for addressing them during the course of an agreement review.

SUMMARY

Export Control regulations present complex and nuanced compliance requirements at institutions of higher education where risk is not evenly distributed across all university settings or activities. In response, University of California (UC) Export Control practitioners have developed and successfully implemented training and processes for UC staff organized as "red flags." The goal is to maximize efficiency of necessary reviews, especially where export control violations are more likely to occur, while recognizing that the persons/units performing these initial assessments are not export control subject matter experts. Once a red flag is identified, depending on the details and if multiple flags are present, there should be coordination and review by the location Export Control Officer (ECO).

This document serves to define and describe common Export Control red flags within an institution of higher education where robust and dynamic academic research takes place.

It is broken down into the following sections:

1. Background
2. Audience
3. Export Control Policy
4. Export Control Red Flags
5. Types of University activities and transactions that should be considered for red flags
6. How to address export control red flags

Understanding that compliance measures add administrative burden, any new or expanded processes or protocols should be evaluated for efficiency, ease of use (for example, simplified and standardized forms and systems) and effectiveness.

1. BACKGROUND

While the policy and regulatory carve out for fundamental research [(NSDD 189), EAR (15 CFR § 734.8) and ITAR (22 CFR 120.11(a)(8))] protect highly collaborative, open and international engagements at higher education institutions like UC, not all university operations or activities meet this exemption. *Some examples of activities that are not exempt* under the Fundamental Research Exclusion (FRE) as outlined in the UC Export Control Policy include:

- Transfer of proprietary information related to controlled items or technology,
- Transfer of ITAR-controlled items (particularly if UC receives ITAR items or technical data),

- Sales and service agreements related to controlled items or technology,
- Physical exports outside the U.S. of hardware, software, or technology,
- Engagements and transactions with restricted parties or entities that are not covered by the FRE,
- Defense services,
- Restricted end uses, or
- Transactions involving embargoed or sanctioned parties/countries.

Given these limitations, specific activities must be reviewed to identify applicability of compliance requirements and ensure implementation of appropriate mitigation measures.

2. AUDIENCE

In most cases, UC staff who negotiate and/or accept sponsored research or other types of institutional agreements are in a position to first recognize and escalate Export Control red flags. As such, this guidance document is primarily targeted to UC staff whose role or responsibilities include oversight of contracts and grants, international agreements, service and sales agreements, non-disclosure agreements, confidentiality agreements, material transfer agreements, technology transfer agreements or intellectual property licenses, and other types of agreements that may bind UC.

How to Use This Guidance:

This Guidance discusses the most common and highest risk red flags within an institution of higher education, as generally accepted and practiced around the country. Due to organizational differences, UC locations should review this guidance with the following next steps in mind:

- Who needs to be aware of Export Control red flags at your location based on each UC member's role and responsibilities? What training exists or must be created to create sufficient awareness?
- Where are the highest concentrations of red flags at your location? This could be around academic departments (e.g. School of Engineering), organized research units, laboratory or specialized facilities, or specific administrative office (e.g. the Vice Chancellor for Research Office or Financial Services).
- What processes or procedures can be implemented to identify Export Control red flags? Consider leveraging existing processes or procedures already in place in specific areas where Export Control red flags can be added. For example, if there is a process or system for Material Transfer Agreement intake, consider adding Restricted Party Screening to identify parties to the agreement that would require review for legal or regulatory requirements.

3. EXPORT CONTROL POLICY

In line with the UC Export Control Policy, Export Control compliance (including the identification and esclation of red flags and restricted party screening), is a shared responsbility across the UC system. The UC Export Control Policy lists the specific groups who share in this responsibility, including Faculty and Other Academic Appointees, Staff, Students and Nonemployee participants in University programs, and export control and compliance officers. See Appendix A for the full list.

4. EXPORT CONTROL RED FLAGS

Keep red flags in mind when reviewing agreements. Close coordination with your location Export Control Office is needed for agreements with Red Flags, especially when multiple are present. Red Flags are organized into the following categories:

- Controlled Technologies
- Country Restrictions
- Sponsor
- Export Control Language
- Physical Exports
- Restricted Parties

A chief goal of export controls is to prevent proliferation of defense or other sensitive technologies that could provide a mililtary or special strategic advantage to foreign governments. UC researchers lead the world in academic research, including cutting-edge areas of science and engineering, which may require use of the state-of-the-art technological tools and information. Oftentimes, it is these technologies that are the most sensitive and, therefore, export controlled.

In general,**controlled technologies** will relate to technology areas and items listed as export controlled [i.e. appearing on the Commerce Control List (CCL) or U.S. Munitions List (USML). Relevant technologies typically involve military, space, nuclear, and similarly sensitive applications. An example of controlled technology that can be utilized within a university research environment is infrared cameras developed for the military but utilized for research on eye disease. The federal government is also moving to add a separate list of technology areas, termed “Emerging Technology,” as broader areas where there is an economic or strategic defense advantage to control proliferation of those technologies. Some examples of Emerging Technologies include:

1. biotechnology
2. artificial intelligence and machine learning
3. position, navigation, and timing (“PNT”) technology
4. microprocessor technology
5. advanced computing technology
6. data analytics technology
7. quantum information and sensing technology
8. logistics technology
9. additive manufacturing
10. robotics
11. brain-computer interfaces
12. hypersonics
13. advanced materials
14. advanced surveillance technologies

This list is not exhaustive and may be updated based on U.S. government priorities and other developments. Locations should provide awareness training on controlled technologies and Export Controls in coordination with their local Export Control Officer.

Like any of the red flags listed here, the existence of a related controlled technology in an agreement or other activity alone does not indicate an export control requirement or risk, but rather a factor that, taken together with other facts, may or may not indicate a risk. The local Export Control Officer can advise further on which controlled technologies or other red flags should be escalated for further review and determination.

Export Control regulations related to controlled technologies, such as those listed on the U.S. Munitions List (USML) and Commerce Control List (CCL), vary based on the country of export. An export can include tangible (physical shipments or transfers) or intangible (data, software or information) exports. Release of controlled information (i.e. "Technology" or "Technical data") to non-U.S. persons is termed a "deemed export." Deemed exports can occur even while the foreign person is inside the U.S. Generally speaking, if an export license is required for a tangible export of a specific technology to a specific country, an export license would likewise be required for deemed exports of that technology (information) to nationals of that country and who have not been granted permanent residency status in the United States.

The Department of Treasury's Office of Foreign Asset Controls (OFAC) also maintains country-based sanctions programs, such as the Iranian Transactions and Sanctions Regulations (ITSR), which strictly control services to Iran, Iranian nationals or individuals located in Iran. Activities such as research collaboration or conference attendance in Iran can require an OFAC license. As such, UC activities involving foreign countries amount to an export control risk.

Risk varies widely based on the country. For example, countries under comprehensive sanctions or with tighter technology controls under the EAR or ITAR are considered higher risk. Your location Export Control Office can determine the **country restrictions** and specific requirements for any country that UC will be engaging.

The highest risk countries, regardless of activity, are those under OFAC's most comprehensive sanctions, including Cuba, Iran, North Korea, Syria and Ukraine (Crimea region). Any activities involving those countries, including field research, travel, conference presentations, collaboration, etc., need to be escalated to your location Export Control Office to determine whether the activity requires a license. Escalation and license review must take place prior to the activity to avoid violations.

The Federal government has placed additional controls on countries with a high level of military-civil fusion, where the private sector is actively involved and compelled to participate in research programs that aid or develop the military. The current list of military end user (MEU) countries include Cambodia, China, Russia, Myanmar (Burma) and Venezuela.

When UC receives funding from or contracts with outside parties, there is inherent Export Control risk, as many **sponsors**, industry partners and other organizations operate outside the Fundamental Research Exclusion (FRE). As such, UC may be contracting with or entering into agreements with parties that are conducting export controlled research or development, using export controlled technology, or otherwise generally limiting access to information or items based on citizenship. However, not all sponsors or partners will carry the same export control risk. In cases where UC is selling a service or other item, those activities do not fall under the FRE and may be subject to export controls. Based on the nature of the activity and red flags, coordination with the Export Control Officer, could be necessary for the sale of service or items.

Generally speaking, a sponsored research project funded by the National Institutes of Health (NIH) for biomedical research carries less export compliance risk than participating in a Department of Defense (DoD) research project. While the DoD regularly funds and encourages basic research projects, where the results will be published in academic journals and there are no disemmination or citizenship restrictions, the intent for the research funded by the DoD likely has a national security or military application further along in the research and development process. In addition to the DoD, other examples of sponsors that may carry additional export compliance risks include:

- U.S. defense, aerospace and intelligence agencies (DARPA, NASA, NSA, etc.)
- U.S. nuclear energy and weapons agencies (DoE, NRC, E-ARPA)
- U.S. defense, intelligence, aerospace and nuclear contractors (Space X, General Atomics, Boeing)
- Foreign defense, aerospace, intelligence and nuclear agencies

Defense Service

Interactions and collaborations with foreign defense, aerospace, intelligence and nuclear agencies, or with foreign non-governmental organizations where the research area relates to defense, aerospace, intelligence or nuclear technology or application, such as defense contractors, may trigger a “defense service.” “Defense services” are regulated under the International Traffic in Arms Regulations (ITAR) to control the provision of services related to “defense articles” (ITAR-controlled military items or technical data) as well as engagements with foreign defense and foreign defense-affiliated organizations and individuals. Prior authorization from the U.S. government in the form of an export license or Technical Assistance Agreement (TAA) from the Department of State is required.

Transfer of Intellectual Property, Technology, Data, Software or Items

Sponsored projects or partnerships may involve the use of proprietary information or intellectual property (IP) not meant for the public domain or the use of proprietary items and software. Such information and items can be received under a nondisclosure agreement or other agreement type where UC agrees to keep them confidential. Information that is not in the public domain or intended to be published as part of academic research does not qualify under the Fundamental Research Exclusion (FRE) and is therefore subject to export controls. In particular, industry partners often intend to protect the trade secrets and commercial value of their information and technology. UC should understand the intent of an industry partner to appropriately assess export control risks.

UC's primary strategy to protect its open and collaborative environment as a fundamental research-focused institution is to ensure that institutional agreements do not contain publication or foreign national restrictions—whether in the agreement terms and conditions or the activities outlined in the project—that would remove UC's qualification for the Fundamental Research Exclusion (FRE).

There are two primary scenarios where **export control language** within an agreement would present an inherent risk to the University:

1) The agreement from the outside party contains export control language that indicates the activity covered by the agreement may require restrictions or approval.

Sponsors and partners whose operations regularly concern export restricted activities or technology typically include export control clauses in their agreements. The clauses serve to ensure compliance with receipt of export restricted items or other specific concerns, or more generally, to guarantee all parties will follow general export control regulations.

Sections containing problematic export control language are often, but not always, marked with a heading containing the following (or similar) terminology: Export Control, Export Controls, Export Compliance, Global Trade Compliance, Anti-terrorism, Sanctions, etc.

When export control relevant language is identified, the location Export Control Office should be contacted for further guidance prior to signing the agreement or moving further into any related activity. Locations may establish processes with the local Export Control Office to escalate only problematic language vs. standard compliance language.

Each location can use its own template export control language in UC generated agreements as long as it meets UC Export Control policy guidance. However, UC export control template language should aim to actively communicate the University's open environment and require partners to inform UC in cases where export controlled information or items will be shared with UC, so that the appropriate steps can be taken to address regulatory or legal requirements before receipt.

University members negotiating incoming agreements with problematic export control language should consider using the location's template export control language. The addition of a notification requirement prior to sharing export controlled information or items with UC is especially recommended for high risk sponsors or partners, as discussed above.

2) Agreements without export control language that protects UC from disclosure of export controlled items or information.

Whether export control language is present in incoming agreements or not, Contract and Grant Officers should, at minimum, consider adding language requiring partners to identify when export controlled items or information will be provided to UC prior to any such disclosure. In cases where such items or information will be provided, the language should also require that the associated export control classification number (ECCN) is disclosed to the location's Export Control Office. Particularly for partners and projects with other export control risks (such as the red flags identified in this guidance), Contracts and Grants Officers should consider adding the location's template export control language to sponsored research awards, NDAs, MTAs, or other

similar agreements.This approach sets the expectation that UC is an open, academic environment and fundamental research focused institution as a default, and any restrictions need to be clearly identified and addressed at the time of agreement. Identification of such restrictions prior to beginning any sponsored projects or partnership is crucial for UC to maintain its openness and facilitate compliance with any legal obligations relating to export controls. This is particularly important when the agreement covers the transfer of items or information to UC.

Apart from sections specifically marked “Export Control” or “Global Trade Compliance,” “Sanctions,” or “Anti-terrorism” that deal specifically with export control regulations, you should also consider export controls in relation to clauses involving:

Publication Review/Approval and Limitations on Participation by Foreign Nationals – The two most common issues with agreements that preclude UC’s use of the fundamental research exclusion are restrictions on publication and foreign national participation. When the sponsor or partner limits UC’s ability to freely publish the results of research or include foreign nationals, regardless of citizenship status, the FRE does not apply. Consult with your local Export Control Officer for guidance.

Proprietary Information – Proprietary Information (such as that received under a non-disclosure agreement (NDA) or confidentiality disclosure agreement (CDA)) or certain types of export or disemination controlled information, cannot be publicly released and is therefore “subject to” export control regulations. Information and data “subject to” export controls must be identified and reviewed to determine if the release of such information to foreign persons during the course of research or other university activities would require an export license.

Data Use, Protection and Cybersecurity requirements – Data Use or Software License Agreements often involve special data or software handling and use requirements. Typically, these requirements intend to protect the unlicensed or unauthorized release or disclosure of these items. Like proprietary information, data or software that cannot be publicly released is subject to export controls, and therefore any related regulatory and legal requirements. Additionally, these agreements often carry specific IT security or controls as part of the agreement terms.

Restricted or proprietary technology inputs and outputs – Most educational and research activities at UC involve published data or activities intended to result in the publishing of data for the scientific community. In certain cases, sponsored research or other activities may require the partner to provide UC with government or company proprietary information where unauthorized public disclosure or disclosure to foreign persons may carry specific regulatory, contractual, or other legal requirements. In research where such restricted or proprietary information is required as an “input,” UC researchers and administration must take special care to address any legal, regulatory and contractual requirements, while considering how the restricted inputs will influence or affect the research results, i.e., the “output.” For example, if a research project is specially informed by restricted information as an input, where the research results could be not have been formed without this information, the resulting research, data or developmental items, including equipment, material, software or encryption, may be restricted in a similar or more restrictive manner as the inputs. The alternative (and ideal case) is a purely fundamental research project where there are no controlled inputs, and there are no restrictions on the publication of results or particapation of foreign nationals on the project.

In order to mitigate this risk, faculty and research administrators must be aware of the potential for this scenario and how to identify restricted proprietary information or technology through common sponsored research and university activities, including but not limited to:

- Non-Disclosure Agreements (NDAs) and Confidentiality Disclosure Agreements (CDAs)
- Data Use Agreements (DUAs) and Software License Agreements (SLAs)
- Partnerships or Sponsorships from high risk government agencies, including the Department of Defense, Department of Energy, NASA and Intelligence Community (IC) agencies

- Partnerships or Sponsorships from industry partners, most notably defense contractors working on Department of Defense or other programs of specific national security concerns

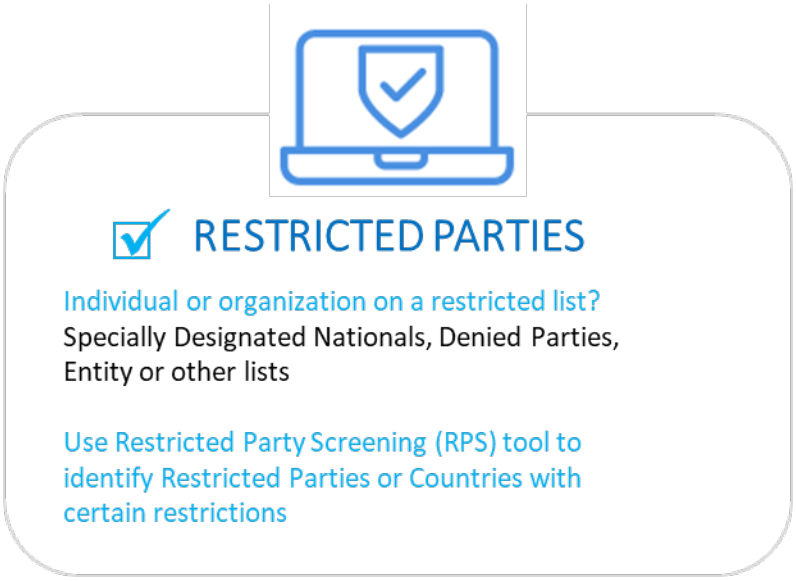
One preferred method of identifying potentially restricted inputs is to include agreement language as a standard practice that requires the third party to positively identify the provision or presence of any information or items that carry restrictions, and to confirm that UC is free to publish research results without prior approval (except for a reasonable delay for the the partner's/sponsor's *review*. It is important to note that it is generally not permissible, under the University of California's publication policy (See Chapter 1-400 of UC's Contract and Grant Manual), to accept terms in research agreements that restrict or require third party approval for publication or dissemination of research results. In cooperation with the sponsored research and compliance offices, locations can craft standard language to include in sponsored research proposals and awards and other agreement types.

Physical exports or transporting items outside the U.S. may require an export license depending on the items and destination country. The act of exporting includes shipments, regardless of method or carrier (FedEx, UPS, DHL, Freight Forwarder), and items hand carried or packed in baggage during travel. Contemplated exports for UC-related purposes or operations (research, education, business, etc.) must be reviewed to determine license requirements prior to leaving the U.S.

At the time of agreement, the university member reviewing the activities to be carried out has an opportunity (perhaps the only one) to identify a future export activity. In sponsored research awards, the proposal statement of work, budget and budget justification may describe intended export activities as part of the research project, such as:

- Field research performed outside the U.S.
- Activities with international collaborations that could involve tangible exports
- Budget line items for international shipping or travel expenses
- Budget justifications discussing costs for international shipping, travel or other activities

Physical exports outside the U.S. represent one of the biggest risks to Export Control compliance, as the regulations are very clear in outlining whether an export requires a license, qualifies for an exception, or does not require a license at all. Special attention and care should be taken in cases where a physical export is identified during an agreement review.



Restricted Parties refer to individuals and organizations on one of several government restricted lists. Restricted Party Screening (RPS) should be performed on international individuals and organizations where UC is entering into a formalized agreement, with limited exceptions (one being matriculated students only taking classes). Engagements with restricted parties are a Red Flag. They may include the receipt or transfer of funds or services, or research collaborations, and carry both potential legal requirements and reputational risks. Consult the UCOP Restricted Party and Entity of Concern Escalation Procedure Guidance for additional detail on creation of a local procedure to adequately identify, analyze and decide on whether to engage with Restricted Parties.

5. TYPES OF UNIVERSITY ACTIVITIES AND TRANSACTIONS THAT SHOULD BE CONSIDERED FOR RED FLAGS

The above is a discussion of Red Flags. This chart outlines how the Red Flags relate to specific agreements and functions.

Agreement type	Purpose	Transfers	Examples	Red flags
NDA or CDA	Transfer of information	Technology (information)	Process Design Kits, “know how,” intellectual property, designs, manuals, blue prints for sensitive items	Sponsor, Agreement language, Controlled Technologies, Restricted Parties
Research Agreement	Financial support for research	Technology, items, software	Funds, know how, intellectual property, materials, equipment	Sponsor, Agreement language, Controlled Technologies, Restricted Parties
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	Sponsor, Agreement language, Controlled Technologies, Physical exports, Restricted Parties
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	Sponsor, Agreement language (it is most important here to stick to your standard language), Controlled Technologies, Restricted Parties

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	Sponsor, Agreement language, Controlled Technologies, Restricted Parties
Material Transfer Agreement (MTA)	Material transfer	Technology, items, software	Material Transfer Agreements or other IP transfer where tangible items and international shipments are involved	Sponsor, Agreement language, Controlled Technologies, Physical exports, Restricted Parties
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	Sponsor, Agreement language, Controlled Technologies, Restricted Parties
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.	Agreement language, Controlled Technologies, Sensitive countries, Restricted Parties

6. HOW TO ADDRESS EXPORT CONTROL RED FLAGS

Once a red flag as outlined in this document is identified, each location and responsible office should evaluate and document a process for escalation and review by the Export Control Officer (ECO). As described in the UC Export Control Policy, the local ECO is

"[R]esponsible for the monitoring and oversight of the local Export Control Compliance program (including regular assessments). ECOs shall be issued appropriate delegations of authority to effectively implement the local Export Control Compliance program. ECOs will serve as the *primary point of contact and subject matter experts* at that location. *The ECOs are responsible for reviewing the applicability of export control regulations and/or determining options for export licensing, exceptions, or control plans to mitigate risk*. As part of the review process, the ECOs consult with the persons involved in the transaction (e.g., researchers or staff) to understand the technology and the specifics of the situation." (Emphasis added.)

In the context of agreement reviews, the relevant areas of responsibility from the policy are emphasized above.

Depending on the transaction, the ECO may consult with the persons involved in the transaction (e.g., researchers or staff) to understand the technology and the specifics of the situation. Apart from the ECO, other stakeholders may be included in the export control review to provide information or guidance outside of regulatory or compliance requirements.