University of Maryland
Export Compliance Program

Message from the University of Maryland, Vice President for Research:

US export regulations are designed to advance the national security, foreign policy, and economic interests of the United States by controlling the transfer of technology from the US to foreign locations and foreign persons. These regulations can apply when physical items are shipped out of the country and when certain technical information are shared with foreign persons both inside and outside the United States. As a leading institution in basic and applied research, the University of Maryland is committed to being a good steward of US investment in research and technology development. An essential component of this commitment is our efforts to maintain a robust Export Compliance Program which oversees our research endeavors to identify and manage activities that are subject to US export control.

The responsibility for direct oversight of our Export Compliance Program has been delegated to the Research Security Office in the Division of Research. The Director of the Research Security Office has the designation of *Export Empowered Official* by the University President. While the Research Security Office has this key oversight role, the responsibility for compliance with the regulations is shared with all University personnel involved in activities and processes that are subject to the regulations. The scope of regulations covered by this Program includes the Export Administration Regulations (EAR) (15 CFR §730-774) administered by Department of Commerce, the International Traffic in Arms Regulations (ITAR) (22 CFR §120-130) administered by Department of State, and active sanctions programs administered by the Office of Foreign Assets Control of the Department of Treasury.

The responsibility for compliance with U.S. export laws is shared between all university personnel. To provide the necessary guidance and tools for compliance, the University's Division of Research has an Export Compliance Program administered by the Research Security Officer. The mission of the Research Security Office is to promote research and an atmosphere of compliance with U.S. export laws in the most efficient and transparent manner possible. The purpose of this document is to define the goals of the Export Compliance Program, define the various roles and responsibilities, and outline the services and guidance provided by the Research Security Officer to the various functional areas.

The Research Security Office and this Export Compliance Program have the full support of Senior Leadership at the University of Maryland.

Gregory F. Ball
Vice President for Research

I. Description of Program

The University of Maryland's Export Compliance Program consists of identifying and mitigating compliance risks at every stage of the research process. The responsibility for compliance is shared with all university faculty, staff, and students involved with activities subject to export laws.   However, functional areas of specific compliance risks are identified here along with the key roles and responsibilities for the faculty and staff having the greatest impact in the compliance process. Due to the ever-changing nature of technology as well as the regulatory climate, the Export Compliance Program is an evolutionary process and the Research Security Officer continuously monitors the campus and external factors to identify areas of highest risk so the appropriate information, resources and tools can be made available to those affected, promoting an ongoing atmosphere of export compliance. This document provides an overall description of the Export Compliance Program but the specific processes may be updated from time to time. The Research Security Office maintains the most current SOPs in an internal document library.

II. Organizational Chart and Responsibilities
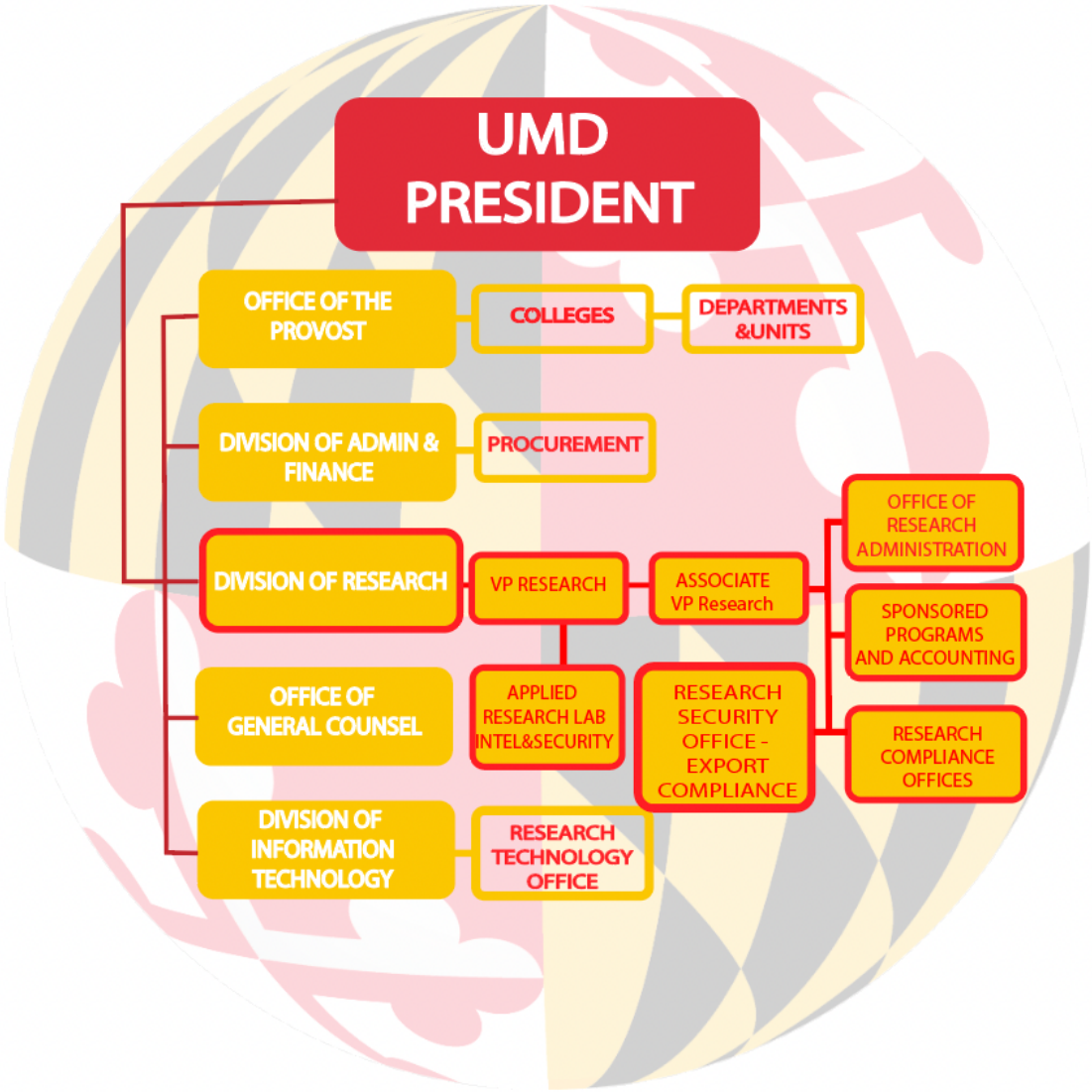
Vice President for Research

The Vice President for Research is the designated Senior Officer for export compliance. The Vice President for Research has undertaken the task to ensure that adequate resources are provided to mitigate export compliance risks at the University of Maryland. The Research Security Officer is funded by the Division of Research and, on at least an annual basis, the Vice President for Research meets with the Research Security Office to discuss the risk landscape and recommendations by the Research Security Officer for policy, guidelines, and resources needed to support an atmosphere of compliance.   The Vice President for Research will also be available on an ad hoc basis to review specific concerns or issues related to export compliance brought forward by the Research Security Officer. The Vice President for Research helps disseminate Research Security Officer guidance to the affected faculty and staff as requested by the Research Security Officer.

Research Security Officer

The Research Security Officer serves as the Export Empowered Official for the University of Maryland and is responsible for managing and administering the Export Compliance Program. The Research Security Officer's primary responsibility is to support research while promoting compliance with export laws in the most efficient and transparent manner possible. Key areas of responsibility include:
- Identifies areas at the University of Maryland that are impacted by export control regulations
- Develops export control procedure guidance to assist the University in remaining in compliance with export control regulations
- Educates inventors, principal investigators, research centers and academic units about export control regulations and procedures at the University of Maryland
- Monitors and interprets export control legislation
- Assists investigators, researchers and offices at the University of Maryland when research involves sponsor restrictions, export-controlled equipment or information by way of a Technology Control Plan
- Provides proposal support to researchers for solicitations involving potential export restrictions
- Seeks advice from the Office of General Counsel in analyzing and handling export control compliance issues
- Applies for export licenses, commodity jurisdiction and commodity classification requests
- Provides support for departments needing to ship items overseas
- Advises and assists with record keeping for export controlled activities at the University of Maryland
- Investigates potential export violations on campus

- Maintains the Research Security Officer website

Division of IT – Research Technology Office

Security of information is closely related to the mission of export compliance. The Research Technology Office will coordinate IT initiatives that may impact the security of export controlled information with the Research Security Officer. The Research Security Officer will also share regulatory information or other information that may impact information security on campus with the IT Research Technology Office.

Export Control and International Compliance Committee

The Export Control and International Compliance (ECIC) committee is a committee, appointed by the Vice President for Research, consisting of a faculty chair, the Research Security Officer, and the liaisons from the Office of Research Administration and the Office of General Counsel, and appointees from affected Colleges. The primary responsibility is to participate in the annual risk assessment meeting and to provide as needed support to the Research Security Officer for the development of guidelines and review of other compliance issues.

Faculty

Faculty members involved in applied research activities with cutting edge technologies (especially technologies with a possible military application) have an increased potential for interaction with export restrictions. Collaborations with foreign entities and especially sanctioned countries such as Cuba, Syria, North Korea, Sudan, and Iran also have an increased potential to be impacted by export restrictions. Faculty possess the most knowledge of the technical scope of their research as well as whether they are in receipt of proprietary technical information furnished by outside sources. For these reasons, faculty have one of the most important roles in the compliance process. Faculty responsibilities include:
- Understanding how their technology (and potential applications) are classified under export laws (The Research Security Officer can provide consultation)
- Understanding whether export laws, including sanctions, may place restrictions on their academic activities (The Research Security Officer can provide consultation)
- Ensuring that accurate information is provided to departmental business administrators to use on Routing Form questions when initiating agreements or proposals

- Understanding and abiding by applicable export laws during international travel
- Ensuring, in consult with the Research Security Officer, that all international shipments are compliant with US export laws
- Abiding by the terms and conditions of their sponsored research agreements
- When necessary, working with the Research Security Officer to establish a Technology Control Plan and properly administering the agreement after execution
- Consulting with the Research Security Officer if they receive any export controlled information or ITAR hardware not covered by a Technology Control Plan or if their sponsor conveys any export control requirements related to their research activities
- Maintaining records associated with export activities in accordance with document retention guidelines herein

Deans/Chairs/Directors/Unit Heads

Deans, Chairs, Directors, and Unit Heads are responsible for promoting an atmosphere of compliance by disseminating key messages from the Research Security Officer to affected faculty and assisting the Research Security Officer in coordinating training activities. Deans, Chairs, Directors, and Unit Heads are also responsible for reviewing and approving Technology Control Plans and understanding the implications and legal risks associated with research involving restricted technology.

Office of General Counsel

The Office of General Counsel reports to the Office of the President at the University of Maryland. The Office of General Counsel will provide a liaison to review the annual risk assessment of the Research Security Officer as well as recommendations, findings, and other matters when requested by the Research Security Officer. Research Security Officer records will be made freely available to the Office of General Counsel, and the Research Security Officer will notify the Office of General Counsel if it becomes aware of any potential violations or enforcement activities on campus related to export laws. To the extent allowable by law and confidentiality provisions, the Office of General Counsel will notify the Research Security Officer if it becomes aware of any potential violations or enforcement activities on campus related to export laws.

Office of Research Administration

Since the greatest potential for export compliance risk areas comes through sponsored research activities, the Office of Research Administration has a key role

in export compliance during their review of proposals and incoming awards for conditions that may require negotiation to remove problematic clauses or a more in-depth export compliance review by the Research Security Officer. The Research Security Officer provides annual training to Office of Research Administration staff on recognizing export compliance concerns. The Office of Research Administration will appoint an Research Security Officer liaison to help coordinate and formulate communications, guidelines, and training efforts with Office of Research Administration staff.

Procurement

Procurement personnel are responsible for reviewing information provided by suppliers and vendors and notifying the Research Security Officer for guidance if any material subject to the ITAR will be shipped to campus or if vendors will be sending proprietary technical data. Procurement terms and conditions contain a clause requiring vendors to notify the University before providing any technology to campus subject to the ITAR. Procurement personnel are also responsible for screening international vendors against restricted party lists and maintaining associated records in accordance with the record retention requirements herein.

Office of Technology Commercialization

Office of Technology Commercialization personnel consult with the Research Security Officer for any contemplated IP licensing activity with foreign parties and anytime non-standard terms are used related to export compliance on licensing or non-disclosure agreements.

Institutional Biosafety Committee

Dual Use Research of Concern (DURC) is defined as *"life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security."*

The US Government policy for DURC can be found at the following site: http://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf

The policy requires institutions conducting research that meet the criteria for DURC to have an Institutional Review Entity empowered to execute the requirements of the Policy. The Vice President for Research has delegated this authority to the Institutional Biosafety Committee. The Research Security Officer will serve as an ad hoc committee member for DURC reviews.

<u>Departmental Business Administrators</u>

Departmental administrators are key liaisons between faculty, the Research Security Officer, and the Office of Research Administration. Departmental business administrators are generally aware of research projects requiring shipping out of the country, collaborations with foreign entities, international travel, and other research activities with potential export compliance concerns.   Typical areas of responsibilities include:

- Consulting with the Research Security Officer for activities with potential compliance concerns
- Assisting the Research Security Officer in identifying areas of risk that could benefit from additional Research Security Officer training efforts
- Ensuring, in consult with the faculty and the Research Security Officer, that all international shipments are compliant with US export laws and any required records are maintained in accordance with record keeping policies
- Ensuring that the individuals completing H-1B screenings and Routing Forms for sponsored research or unfunded agreements have attestations from the appropriate faculty members as to the accuracy of the information

Departments with significant export related activities may appoint an Export Liaison to receive direct training from the Research Security Officer. The Research Security Officer works with the Export Liaison to help facilitate a process for quick review of activities with export compliance concerns.

III.   Overview

The Research Security Officer has established export compliance processes for activities on campus identified as having elevated export compliance risks. This document will only be updated for significant changes in process or policy. The processes described here are not intended to cover every export compliance scenario on campus and it is the responsibility of all faculty and staff to recognize situations that may require specific consultation with the Research Security Officer.

Office of Research Administration

The process of reviewing sponsored research for export compliance concerns starts with faculty and departmental administrators because they have the greatest understanding of the funding opportunity and potential scope of work. The Office of Research Administration routes all proposals, for funded and unfunded agreements, with questions designed to help the Office of Research Administration and the

Research Security Officer identify projects that should have an additional review by the Research Security Officer to determine if there are any conditions requiring additional risk mitigation procedures. Additional information about the process for reviewing proposals and awards is in Section IV.

ORA Post-Approval Monitoring

RSO regularly reviews recent awards to ensure that the Office of Research Administration has documented an export control review for all awards, funded and unfunded, in Kuali. RSO maintains documentation of its review of export-control holds. Additional information on ORA Post-Approval Monitoring is in Section IV.

UM Ventures

UM Ventures refers agreements with foreign entities, including requests through the UM Ventures Store, to RSO for review and restricted party screening. UM Ventures also refers to RSO agreements that indicate export-controlled information will be shared with UMD, and agreements involving UMD technology that may have military or intelligence applications. Additional information about the process for reviewing agreements with foreign entities in Section IV.

University of Maryland Foundation Gifts

The University of Maryland Foundation refers gifts from foreign individuals and other entities to RSO for review and restricted party screening. Additional information about the process for handling foreign gifts is in Section IV.

Procurement and Business Services

Procurement and Business Services refers all agreements with foreign entities to RSO for review and restricted party screening. For agreements that involve exporting items overseas, other than those that are publicly available, Procurement routes an International Shipping form to RSO. RSO also reviews agreements with non-standard export control language. Additional information about the process for handling Procurement agreements is in Section IV.

Restricted Research Waivers

University System of Maryland policy prohibits UMD from accepting research projects whose results cannot be published without sponsor approval, unless the UMD President approves a waiver to this policy. RSO coordinates restricted research waivers for awards whose sponsors will not remove publication restrictions. Additional information about Restricted Research Waivers is in Section IV.

Academic Agreements

The Office of International Affairs refers MOU's and other similar academic agreements to RSO for restricted party screenings. RSO also ranks these agreements according to risk level, based on what the other party is and the activities anticipated under the academic agreement. Additional information about the process for reviewing academic agreements is in Section IV.

Technology Control Plans

The RSO requires a Technology Control Plan (TCP) for projects that involve access to export-controlled technology. Because the sensitivity of technology, individuals involved, and complexity of the project can vary significantly from project to project, the control requirements can vary from one to another. The RSO reviews each project and determines the appropriate TCP controls on a case-by-case basis. Additional information on TCP's is in Section IV.

Foreign Scholar Screening Requests

All foreign nationals who will have UMD appointments, whether staff, faculty, or students, are required to be screened by RSO. RSO screening is required for unpaid appointments. RSO does not screen students who are foreign nationals without appointments. Additional information about Foreign Scholar Screening Request is in Section IV.

IV.   Unit-Specific SOP's

Office of Research Administration

 BACKGROUND:

US export compliance laws control the sharing of sensitive items and technologies with foreign individuals, and foreign entities. Sponsored research activities can have increased risk especially when sensitive technology is involved or when the sponsor or collaborator is a foreign entity.

ORA is the "gatekeeper" of incoming sponsored research and compliance concerns should be identified and addressed before an award is accepted. This plan identifies the process for reviewing incoming awards for export compliance concerns that need to be referred to the Research Security Office (RSO) for further review.

The RSO can help negotiate export control requirements and, when required, will work with the PI and research team to manage the export control requirements of a particular grant or contract.

PROCESS OVERVIEW:

The process starts when the PI completes the proposal questionnaire in KR which is intended to help identify conditions (below) that require an export review. The RSO is not involved in proposals unless the sponsor or solicitation requires special certifications pertaining to security or export control. After a draft award is received, the ORA administrator reviews the KR questionnaire and award draft for conditions (below) which require an RSO review. When conditions are found, the ORA administrator adds the associated hold in the Compliance tab of Institute Proposal and requests an export review from the RSO. The RSO will review and follow-up with the ORA administrator. **If no conditions are found, the ORA administrator must update the Compliance tab to confirm that no Conditions were found by using the *Export Control [Internal]* flag and the UM Approval Not Required status.** This serves as the ORA administrator's certification that an export review was completed without the RSO's involvement.

CONDITIONS REQUIRING EXPORT REVIEW:

- Foreign sponsors, collaborators, subawards
- DOD contracts (Grants only if there are other concerns discussed here)
- Projects where UMD will be receiving confidential technical information furnished by an industry or government source unless the clause prohibits exchange of export controlled information without further authorization from UMD
- Contract (or any type of agreement) terms invoking export compliance controls (other than "the parties shall comply with applicable laws…")
- Clauses invoking specific IT security requirements.
- Shipping materials to foreign countries
- Restrictions on open publication of research results (i.e. sponsor approval required or university research results are "proprietary")
- Restrictions on foreign researcher participation in research projects
- Agreements with terms requiring boycott of services or products of a specified foreign country

PROCESS DETAIL: (See process flow graphic below for visual representation)

ALL incoming research awards require a basic export review by the ORA administrator BEFORE award acceptance. An RSO review is only required when one or more of the above conditions are identified during the review process.

A) **Proposals:**
   1) ORA CA reviews questionnaire for "yes" responses on export control questions and adds the associated *Special Review* hold (see Table 1).
   2) Proceed with proposal submission process.
      Note: CA may send proposal and solicitations to RSO for ad hoc review if obvious export concerns are identified or if the sponsor or solicitation arequires special certification related to export or security requirements.

B) **Incoming Awards/Notice of Awards:**

1)   Review (again) questionnaire responses in Proposal Development to ensure proper holds are added in the Compliance tab of the Institute Proposal (see Table 1).

2)   Review draft contract and SOW for Conditions requiring export review in the list above.

3)   If, after reviewing the routing questions, Compliance tab, and the contract or grant documents, no *Conditions Requiring Export Review* are identified, the CA or the AD can update the approval status of <u>*Export Control [Internal]*</u> to <u>*UM Approval Not Required*</u> and proceed with award acceptance. **By selecting <u>UM Approval Not Required</u>, you are certifying that you have completed an export review and no *Conditions Requiring Export Review* have been identified.**

4)   If one or more *Conditions Requiring Export Review* are identified, proceed with the following actions as applicable:

a.   *Export Control-Collaborator*: Send the IP#, name of sponsor, name and address of foreign parties (including sponsor or subawardees if foreign) to export@umd.edu for screening and approval.

b.   *Export Control* – [All Others]: Send a description of the hold, the draft contract documents, along with the IP# to export@umd.edu for review and approval.

Note: use "URGENT" or "TIME SENSITIVE" in the subject line when there is a specific deadline. Call or Text Adam or Elizabeth if something is REALLY URGENT.

5)   The RSO review can happen in parallel with other negotiations with sponsor but **hold on award acceptance** until the Research Security Office has ***Approved*** all export holds. Under urgent deadline situations, an Assistant Director may allow an award to be accepted with a pending export hold but the Account shall not be created until the Research Security Office has reviewed and ***Approved***.

C)   Post Award Modifications/New Subawards:

1)   Review any requested modifications for changes in scope that might create one or more new ***Conditions Requiring Export Review***. Send a description of changes and a copy of the draft modification to export@umd.edu for review prior to accepting the change.

2)   New foreign subawards (that were not reviewed and approved by the Research Security Office during the pre-award phase) must be submitted to the RSO for approval prior to award. Send the name and address of the subaward recipient, along with the KFS account number, to export@umd.edu.
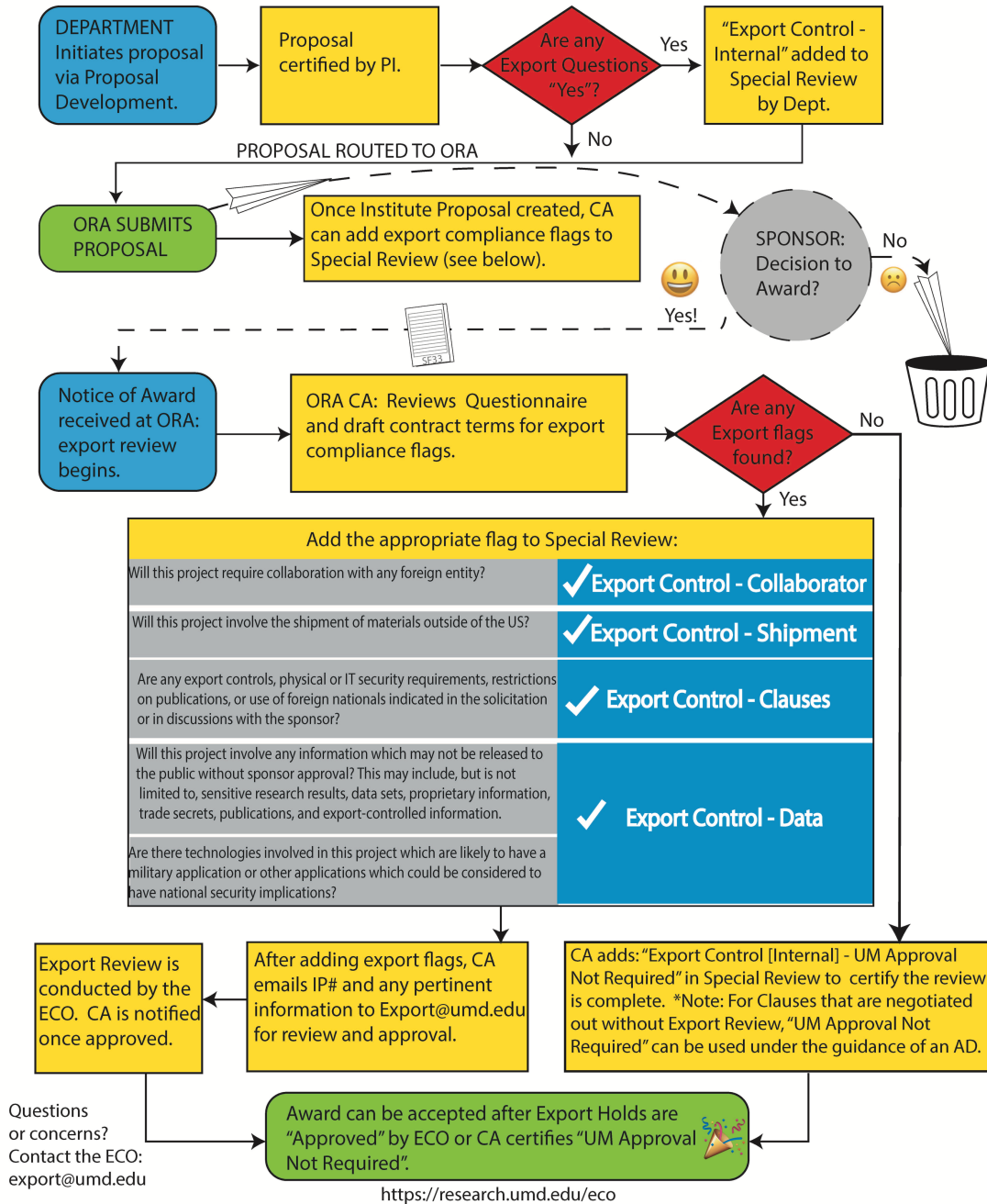
Table 1: Export Questions in Questionnaire and Associated Compliance Tab Hold

Questionnaire Question	Compliance Tab Hold
None answered yes	Export Control [Internal]

|	
Will this project require collaboration with any foreign entity?	Export Control - Collaborator
Will this project involve the shipment of materials outside of the US?	Export Control – Shipment
Are any export controls, physical or IT security requirements, restrictions on publications, or use of foreign nationals indicated in the solicitation or in discussions with the sponsor?	Export Control - Clauses
Will this project involve any information which may not be released to the public without sponsor approval? This may include, but is not limited to, sensitive research results, data sets, proprietary information, trade secrets, publications, and export-controlled information.	Export Control - Data
Are there technologies involved in this project which are likely to have a military application or other applications which could be considered to have national security implications?	Export Control - Data

OFFICE OF RESEARCH ADMINISTRATION EXPORT COMPLIANCE REVIEW PROCESS

DEPARTMENT Initiates proposal via Proposal Development.

Proposal certified by PI.

Are any Export Questions "Yes"?

Yes → "Export Control - Internal" added to Special Review by Dept.

No

PROPOSAL ROUTED TO ORA

ORA SUBMITS PROPOSAL

Once Institute Proposal created, CA can add export compliance flags to Special Review (see below).

SPONSOR: Decision to Award?

No

Yes!

Notice of Award received at ORA: export review begins.

ORA CA: Reviews Questionnaire and draft contract terms for export compliance flags.

Are any Export flags found?

No

Yes

Add the appropriate flag to Special Review:

Question	Flag
Will this project require collaboration with any foreign entity?	✓ **Export Control - Collaborator**
Will this project involve the shipment of materials outside of the US?	✓ **Export Control - Shipment**
Are any export controls, physical or IT security requirements, restrictions on publications, or use of foreign nationals indicated in the solicitation or in discussions with the sponsor?	✓ **Export Control - Clauses**
Will this project involve any information which may not be released to the public without sponsor approval? This may include, but is not limited to, sensitive research results, data sets, proprietary information, trade secrets, publications, and export-controlled information.	✓ **Export Control - Data**
Are there technologies involved in this project which are likely to have a military application or other applications which could be considered to have national security implications?	

Export Review is conducted by the ECO. CA is notified once approved.

After adding export flags, CA emails IP# and any pertinent information to Export@umd.edu for review and approval.

CA adds: "Export Control [Internal] - UM Approval Not Required" in Special Review to certify the review is complete. *Note: For Clauses that are negotiated out without Export Review, "UM Approval Not Required" can be used under the guidance of an AD.

Questions or concerns? Contact the ECO: export@umd.edu

Award can be accepted after Export Holds are "Approved" by ECO or CA certifies "UM Approval Not Required".

https://research.umd.edu/eco

ORA Post-Approval Monitoring

1.) Each month, you will need to run a report for the dates you would like to audit. To do this in Tableau, please see below. You must be on campus or logged into the VPN to run reports in Tableau.
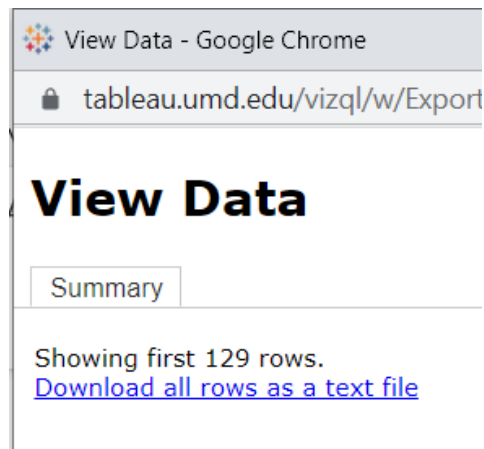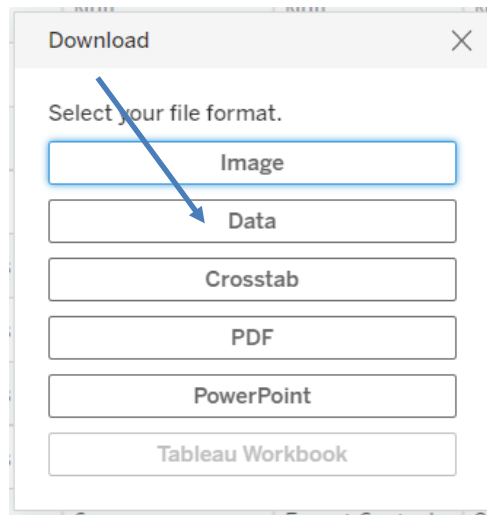
Navigate to the [Export Control report](#).
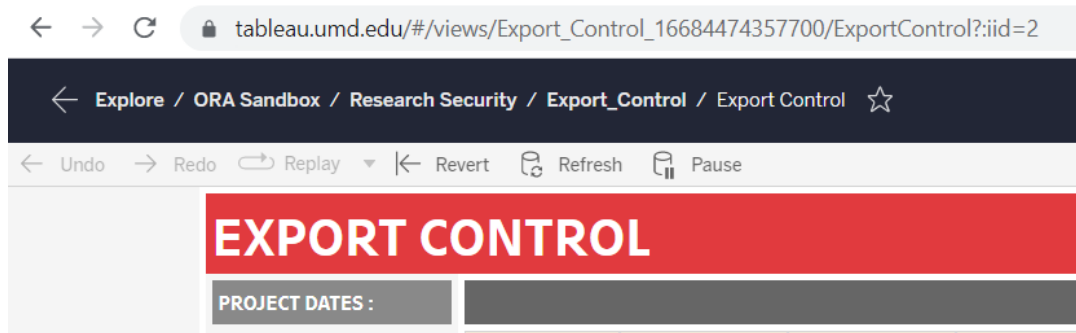
- Change the Start Date to the first day of the month you are auditing.
- Under Special Review Type, uncheck All, and check the following:

ing Download, then Data, then
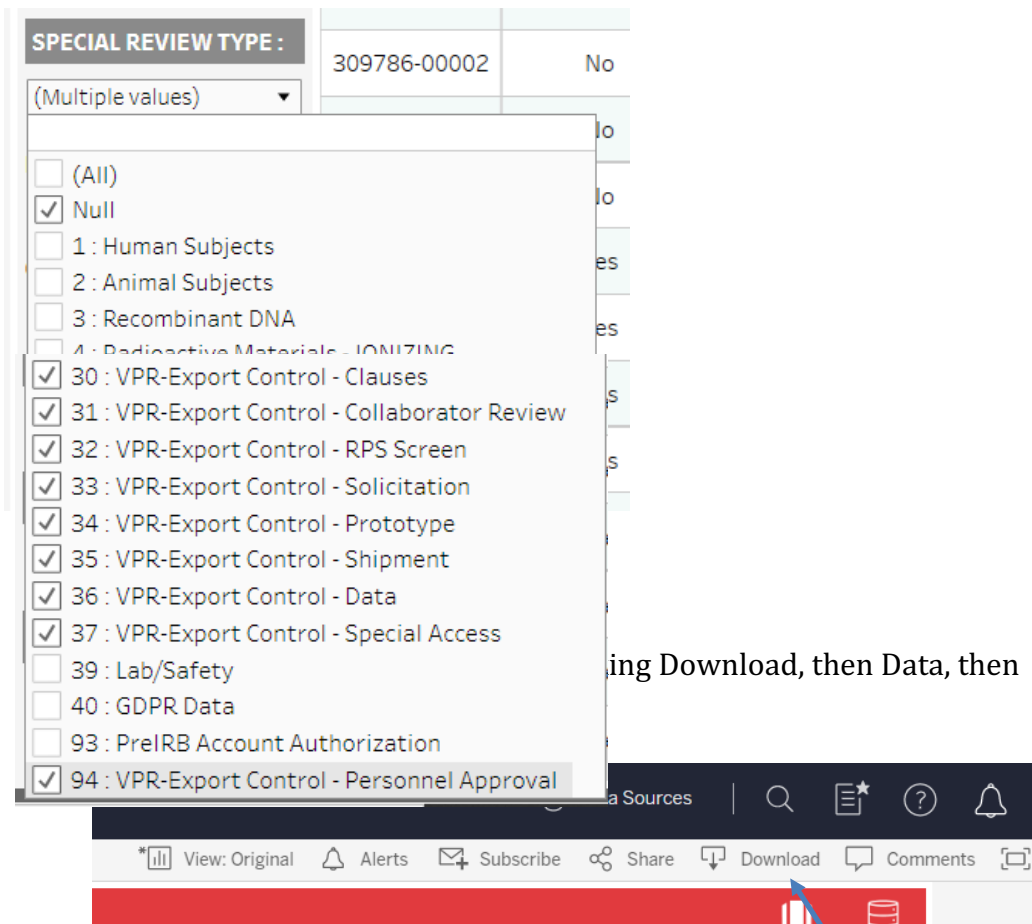
2.) Once you generate the Excel version of the Tableau report, delete the following awards.

- Awards with start dates after the month you are auditing. You will need to do this outside Tableau because the Export Control report in Tableau does not allow you to set an end date.
- Child awards, which are awards other than ######-00001.

3.) Save the filtered Excel version of the report at Box\ECO Server\Post Approval Monitoring\ORA Monitoring\[FY##].

4.) Review the spreadsheet and highlight in yellow any awards that present an obvious export control flag. This should include all awards missing an Export

Control hold, along with DoD-funded awards, SBIR/STTR awards, and awards with foreign sponsors. Each month, select approximately 15 projects for an audit.
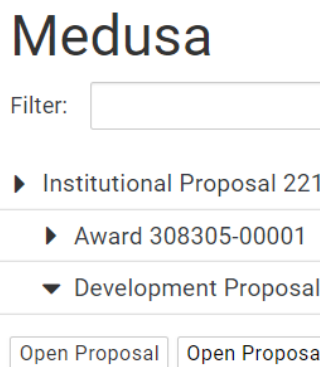
5.) In Kuali, find the first highlighted project on the list by clicking Search Records on the left, then searching by award number.
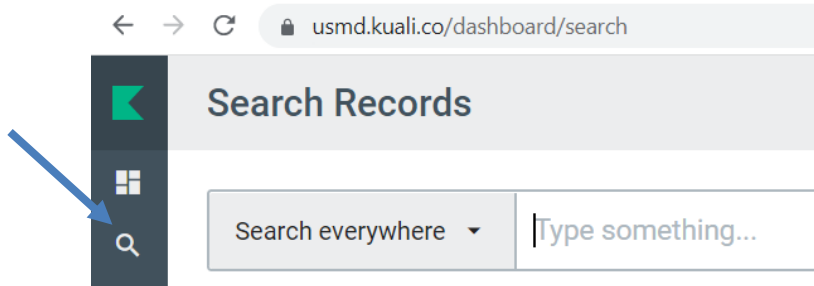
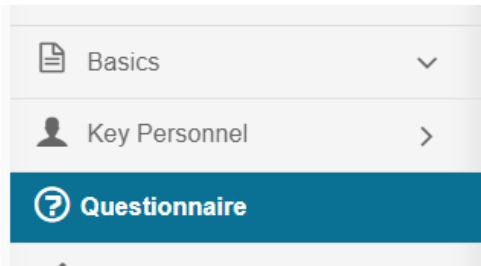- Click on the hyperlink to navigate to the Award.
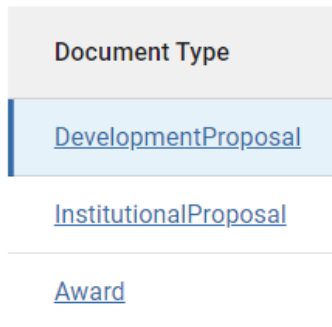
- In the Award, go to the Medusa tab at the top of the screen, then click on Development Proposal, then Open Proposal.

- In the Proposal, click on Questionnaire, then scroll down to the five questions related to export controls. In the audit report, record the answers, yes or no, to each of the five questions.

Are any export controls, physical or IT security requirements, restrictions on publications, or use of foreign nationals indicated in the solicitation or in discussions with the sponsor? ⓘ
No

Are there technologies involved in this project which are likely to have a military application or other applications which could be considered to have national security implications? ⓘ
No

Will this project involve the shipment of materials outside of the US? ⓘ
No

Will this project require collaboration with any foreign entity? ⓘ
No

Will this project involve any information which may not be released to the public without sponsor approval? This may include, but is not limited to, sensitive research results, data sets, proprietary information, trade secrets, publications, and export-controlled information. ⓘ
No

6.) Return to the Award, and, if an Export Control hold has an Approval Status of Approved, enter the date of approval in the audit report. RSO approval may be via e-mail or via other internal approvals such as TCP's.


7.) Still in the Award, click on the Comments, Notes & Attachments tab, then click Show to see the Attachments.
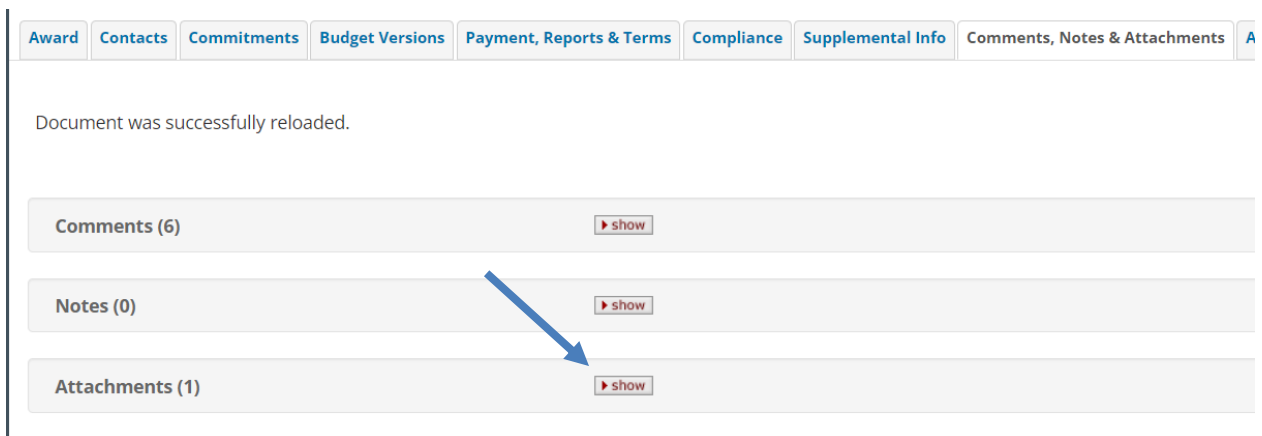
- Click View to see the award, then read the award for any terms related to export control. If there are any terms that require RSO review, there should be a corresponding Export Control hold in the Award, regardless of responses in the Proposal questionnaire.

8.) Still in the Award, click on the Comments, Notes & Attachments tab, then click Show to see the Comments. Note in the audit report who in ORA set up the award, and whether this is the person who would normally handle this award.
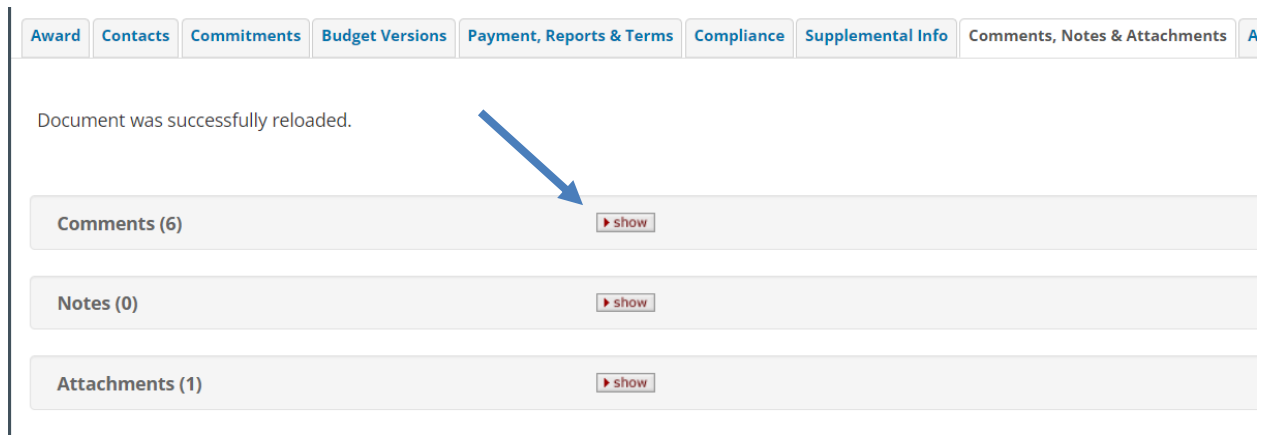
9.) In the audit report, indicate whether the Export Control hold(s) in the Award are correct. If not, note what the hold(s) should be. ARLIS awards, except those with work on campus, need only a VPR-Export Control – Clauses, with approval assumed.

10.) Repeat steps 5 through 9 for all highlighted projects and update the audit report accordingly.

11.) For awards with missing or incorrect Export Control holds, contact the CA who set up the award and ask the CA to correct the Export Control hold in the Award. RSO does not have the Kuali approval authority to update Awards. Send the audit report results to the RSO Director, noting which awards you have asked CA's to fix, and which awards now need RSO review.

UM Ventures

BACKGROUND:

US export compliance laws control the sharing of sensitive items and technical information with foreign individuals, foreign companies, and foreign countries. In general, UMD research that is non-proprietary is not subject to US export laws but

information that is proprietary, unless it will eventually be published in open literature or a patent application, might be considered "export-controlled". Depending on how sensitive the export-controlled technology is, an export license from US Department of State or Department of Commerce may be required. The UMD Research Security Office should review all agreements with foreign entities and domestic agreements when sensitive technologies are involved. The process below is provided by the Research Security Office to support UM Ventures staff when reviewing transactions involving sensitive technologies.

PROCESS:

The following scenarios should be referred to the Research Security Office (export@umd.edu) for review as soon as possible and before the agreement is executed by UM Ventures:

1) All agreements with a foreign entity.
2) Domestic and foreign agreements with terms indicating that export-controlled information will be shared with University personnel.
3) Domestic and foreign licensing activity where university technology may be used in sensitive applications (military or national security significance).

University of Maryland Foundation Gifts

Instructions for Screening of Foreign Gifs:

Submit to Research Security Office (export@umd.edu):

1) name and address of the donor
2) gift letter
3) PI or dept receiving the gift

The Research Security Office will run a restricted party screening of the individual/entity and verify that the gift letter contains no deliverables or other restrictions.

Procurement and Business Services

US export regulations control the transfer of goods, services, and technologies out of the US and, in some cases, can apply to the transfer of technical information to a foreign person. Since procurement usually involves transfer of goods and technologies within the US or to the US, most procurement activities are not subject to export laws but there are a few exceptions. In order to prevent violations, which can have severe penalties for the exporter, the UMD Research Security Office

reviews procurement transactions when conditions are present that have an increased risk of export control violations.

Procurement activities with any of the following situations should be sent to the Research Security Office (export@umd.edu) as soon as possible and **before a contractual commitment is made**:

1) Foreign vendor: US export regulations restrict transactions with certain countries and entities. The Research Security Office will verify that the parties involved in a foreign transaction are not subject to any US sanctions or prohibitions. To request a foreign vendor screening, send the item and vendor details, name of the PI/requesting unit, and any other relevant information to export@umd.edu. "Foreign vendor screening" should be used in the subject line, and "Time Sensitive" or "Urgent" can be used to help expedite the process. Most simple transactions can be approved by the same or next business day.

2) Foreign shipment: All shipments from the US to foreign locations are subject to export control regulations and, in some cases, the US Department of State or the US Department of Commerce must approve an export via an export license before the items leave the US. All foreign shipments for other than publicly available informational materials should be sent to the Research Security Office for an export review as soon as possible to avoid export violations or delays in shipments. In some cases the Research Security Office may need to apply for an export license which can add one or more months to the process. Procurement staff may refer the PI or responsible unit to the International Shipping page and form which will go directly to the Research Security Office or Procurement staff may email the Research Security Office (export@umd.edu) and request a review. The Research Security Office maintains the review records and can provide verification to Procurement staff upon request. International shipping requires specific forms including a customs invoice, packing list, shippers letter of instructions, and an EEI filing for shipments exceeding $2,500. It is the responsibility of the shipper to ensure the records are accurate and complete and to retain the records for five years. Upon request, the Research Security Office can assist with creating and storing the records.

3) **Specific export compliance terms** in the vendor agreement that might indicate that the deliverable is subject to the International Traffic in Arms Regulations (military technologies) or other non-standard export language should be referred to the Research Security Office for review. General statements of "compliance with laws" that are not specific to the item being purchased do not need to be reviewed by the Research Security Office.

Example of clauses requiring review:
This order includes items subject to export control under the International Traffic in Arms Regulations.

Access to items must be restricted to US persons and items shall not be exported without prior authorization from the US Department of State.

Example of a clause that does not require review:
The parties shall comply with applicable export control laws.

Restricted Research Waivers

BACKGROUND:

University policy IV-2.20 – POLICY ON CLASSIFIED AND PROPRIETARY WORK prohibits the university from accepting sponsored research or service contracts which "bar investigator(s) from publishing or otherwise disclosing findings publicly" unless a waiver is approved by the university president. This policy applies to any project with a Classified component and any Unclassified project which contains a term preventing the researchers from publishing their findings unless an approval is obtained by the sponsor. These types of restrictions typically come up in sensitive projects sponsored by security agencies or the Department of Defense. This document describes the process ORA will use to identify and process agreements that contain restrictions which would trigger this policy.

REVIEWING INCOMING SRAs:
- Any indication that the project will have a Classified component
- Any term or clause requiring sponsor to "approve" any data that will be released into the public domain. The most common example of this type of clause is found in DOD contracts: DFAR 252.204-7000. Search the agreement for terms such as "publication" and "dissemination of information".
- Any term or clause indicating that the research or testing results will be considered "proprietary" to the sponsor.

PROCESS ONCE RESTRICTIONS ARE IDENTIFIED:

1. When any of the above conditions are identified, add a Special Review hold in KR: VPR-Export Control – Data and notify the Research Security Officer for awareness purposes.
2. For restrictions involving security Classifications – first contact the PI and ask whether the project scope was intended to include Classified work.   For ARLIS projects, the CA who handles ARLIS (or designee), will verify that the work is within the scope of ARLIS's waiver and the security requirements are in place.
3. For non-ARLIS projects, if the restriction was not expected or planned for in the proposal, you can attempt to negotiate out the restriction. Work with the PI and the Research Security Officer to draft a request for "fundamental research determination" which will need to be approved by the Government

PCO. When the Research Security Officer is unavailable, an Assistant Director should be looped into this process. For non-government sponsored research, the publication restriction needs to be removed from the contract.

4. If the PCO provides a written fundamental research determination, notify the Research Security Officer. The Special Review "Data" hold can be marked "Approved" and a reference to the PCO's written determination should be added to the comment field.
5. If the PCO does not agree, meaning the project is determined to NOT be fundamental research, the Research Security Officer (or ORA Director) will work with the PI and Dept to determine whether to pursue a waiver from the president and initiate the process.
6. In some cases, the president will grant "blanket waivers" that applies to multiple projects or task orders under an indefinite delivery indefinite quantity (IDIQ). Even if a blanket waiver may apply to this project, the Research Security Officer (or ORA Director or her designee for ARLIS) will still need to make a determination that the project is approved under the waiver. A form is used to add new projects and new researchers to an existing project.
7. Once a project waiver is "approved", a "Publication Restriction Waiver" is added in Special Review and the Waiver number is added to the "Protocol" field.
8. The Research Security Office is responsible for tracking approved waivers and providing annual reports to the UMD president.

Academic Agreements

PURPOSE:
International collaborations are an essential component of the University of Maryland's mission and values. When considering international partners and collaborations, it's important to assess whether the activity is in furtherance of the University's mission. This includes identifying any potential legal risks or other ethical or reputational concerns. The following questions should be considered:
- Is the activity in furtherance of the University's mission?
- Is there any potential for adverse national security impacts? (example: providing technical assistance to a foreign country that could be applied to military technology development)
- Could the activity create any legal or risks for the University, University personnel, or students?
- Does the potential foreign party have any accusations or charges of ethical misconduct?
- Is there any risk of adverse reputational impacts that could come from this activity?

This document identifies the due diligence and decision-making process used by University administration to evaluate proposed agreements with international entities.

SCOPE:

This Process is intended to cover academic and research agreements. The University President has delegated the authority to approve academic agreements to the Provost and research agreements to the Vice President for Research. Typical academic agreements include institutional affiliation agreements, academic MOUs, student and faculty exchange agreements, and visiting scholar agreements. Typical research agreements include sponsored research contracts and grants, data-use, material transfers, non-disclosure, teaming agreements, service agreements, and consortium agreements. In some cases, the authority to approve these agreements has been delegated to central administrative units. This process will require some agreements with elevated risks to be escalated to senior administration for a final decision.

PROCESS:

This vetting process may occur in parallel to standard unit processes and should generally occur as soon as practical when considering international agreements. The RSO will conduct the initial screening. For sponsored research agreements, the vetting is incorporated into the Office of Research Administration contract review process. For academic agreements, the review is typically initiated by the Office of International Affairs and done in coordination with the RSO.

Once the request has been received by the RSO, an initial screening of the foreign party is done using a subscription database of all US and foreign parties with specific sanctions under US law. The RSO will conduct a review of the activity and categorize the activity as "Low", "Medium", or "High" risk based on the criteria in the Foreign Agreement Vetting Risk Matrix (see below). Agreements with a Medium or High-risk are escalated based on the Foreign Agreement Escalation Process flow-chart (see below). For Medium or High-risk agreements, the RSO will first work with the initiator to conduct a more thorough risk assessment. If the initiator wishes to proceed with the agreement, the decision is further escalated. If any individual in the escalation chain decides not to proceed, the decision is not escalated further. Medium-risk agreements can be approved at the college-level and High-risk agreements must be approved by the Senior Risk Group consisting of the Provost, VP General Counsel, and VP Research. Records are maintained by the RSO.

Foreign Agreement Vetting Risk Matrix

			Organization Types		
			A	B	C
			-Universities and educational institutions -NGOs/non-profits/other humanitarian/environmental -Basic and applied research organizations (i.e. CERN) -Research funding agencies	-Other government agencies -Tech Industry -Developmental research organizations -Space technology research entities (spacecraft, satellites, sensors, etc.)	-Foreign Ministries of defense and affiliated entities, including universities -Entities involved in the development of defense technology -Police and security organizations -Legal indictments or convictions -Entities with accusations of ethical misconduct, human rights violations, other moral concerns -Countries/entities w/ active US sanctions/prohibitions
Activity Type	A	-Educational exchanges -Academic services (i.e. customized education and training programs, sponsored courses, etc.) -Non-STEM research -Basic STEM research	LOW	LOW	HIGH
	B	-Joint programs, institutes, centers -Non-STEM research in military or security related topics (i.e. START) -Applied STEM Research*	MEDIUM	MEDIUM	HIGH
	C	-Applied STEM research in technology areas that could have military or security applications* -Developmental technology research*	MEDIUM	HIGH	HIGH

*Approval from the Export Compliance Office required for technologies subject to US export control laws

Foreign Agreement Escalation Process

Academic Agreements
Office of the Provost

-Institutional Affiliation
-Academic MOUs
-Student/Faculty Exchange
-Visiting Scholar

Research Agreements
Division of Research

-Sponsored research
-Data use, MTAs, NDAs
-Research MOUs
-Teaming agreements
-Service and testing
-Consortium agreements

This review should be requested early in the process before commitments are made.

Does the agreement include a non-US entity?

YES →

NO →

EXPORT COMPLIANCE OFFICE (ECO)
1) Restricted party screening
2) Risk Matrix Category

HIGH | MEDIUM | LOW

PROCEED WITH STANDARD PROCESS.

MEDIUM RISK ESCALATION FLOW

Approvals can not be delegated to lower-level admins.

PI → YES → UNIT HEAD → YES → DEAN (in consult with OGC) → YES → Notification Provost/VPR/GC

NO | NO | NO

(NO =DECLINE AGREEMENT)

HIGH RISK ESCALATION FLOW

PI → YES → UNIT HEAD → YES → DEAN (in consult with OGC) → YES → Senior Risk Group (Provost, GC, VPR) → YES → Notification Office of the President

NO | NO | NO | NO | SPLIT

PRESIDENT → YES

NO

Additional Considerations for Incoming Technical Data and Restricted Hardware

When export flags are identified for incoming proprietary technical data and incoming hardware, the Research Security Officer will review to determine whether export-controlled information or material will be received. For the initial screening, the Research Security Officer relies on the information furnished by the department to determine if a more comprehensive assessment is needed.

If any of the export compliance questions is answered "Yes," the Research Security Officer will review the activity in more detail to determine if the agreement may involve a deemed export of a restricted material.

Technology Control Plans

Types of TCPs

Individual TCP: In certain cases, UMD personnel may require temporary access to controlled information where a full version of the TCP is not warranted. Examples include working on a proposal with industry collaborators, participating in program meetings with government or industry where controlled information may be discussed or presented, and attending DoD conferences that are not open to the public. In some cases, projects involving technology at a lower control level (i.e. CCL), can utilize this version at the discretion of the RSO. Any legal or contractual security requirements that indicate additional controls may require a Project TCP. The RSO approves the Individual TCP after citizenship verification and after any training requirements are satisfied.

Project TCP: A Project TCP is generally used for research collaborations where more than one researcher will be accessing or creating export-controlled technology. In setting up a Project TCP, the RSO reviews the scope of work, the control level of technology, and any contractual security requirements, and works with the PI to create a customized plan with the controls required by the project. The RSO works in coordination with DivIT and other providers when projects invoke NIST 800-171 IT security standards or other similar standards.

Elements of a TCP

After reviewing a requirement to access controlled information, the RSO determines the appropriate controls based on factors such as the level of access required, technology involved, whether there are physical prototypes, the extent to which external collaborators are involved, and any contractual requirements. The following control elements are considered when setting up a TCP.

> **Access Controls:** Export-controlled technologies are often restricted to US persons or nationals of certain countries. The RSO reviews the scope and

works with the PI as needed to determine the level of restrictions applicable to project technology. The RSO verifies citizenship when adding individuals to Individual and Project TCP.

Physical Security: Projects involving physical prototypes or other tangible items that are export-controlled may require special security controls to limit physical access to the items. Due to the wide range of facilities on campus, the physical security plan will be customized to each project and facility. In some cases, the controlled items can be temporarily accessed in uncontrolled spaces as long as visual inspection will not reveal any sensitive technology and the items are properly secured when not under supervision. More sensitive technologies where visual access could reveal sensitive information may require an access-controlled location. These determinations are made by the RSO on a project-specific basis.

IT Security: Projects that require accessing or generating controlled information require a plan for protecting the files while processing, in transit, and at rest. Projects involving highly sensitive information such as Controlled Unclassified Information (CUI) and Covered Defense Information generally require systems that are administered by a service provider such as the CUI-Environment managed by DivIT. In such cases, the service provider manages the System Security Plan (handles the hardware and software administration and the RSO handles the end-user requirements.

Training requirement: An export control training or briefing is required for individuals accessing controlled information under all UMD Individual and Project Plans. The training can be either in-person, virtual, or recorded at the discretion of the RSO . For more complicated and higher risk TCPs, the RSO prefers an in-person or virtual meeting with the PI and research team.

Post-approval monitoring: More complicated and higher risk projects may warrant additional oversight after a TCP is approved. Oversight may include post-approval meetings, CUI-E usage audit, post -TCP debrief, or effort-reporting verifications. The RSO determines whether a project warrants post-approval monitor when creating a TCP. Monitoring events are scheduled on the RSO calendar.

Creation of the TCP

A TCP is initiated when either a researcher contracts the RSO because they have a need to access controlled information, or ORA has flagged an incoming sponsored research project for potential export controlled activities. The RSO, in consultation with the PI and/or sponsor as needed, will determine whether the project requires a TCP, what type, and what security elements are necessary. With input from the PI and DivIT (if needed), the RSO then drafts the TCP. Once everyone has agreed to the TCP's language, the RSO routes the TCP for the required signatures.

Completion of training and citizenship verification must occur before an individual is added to a project.
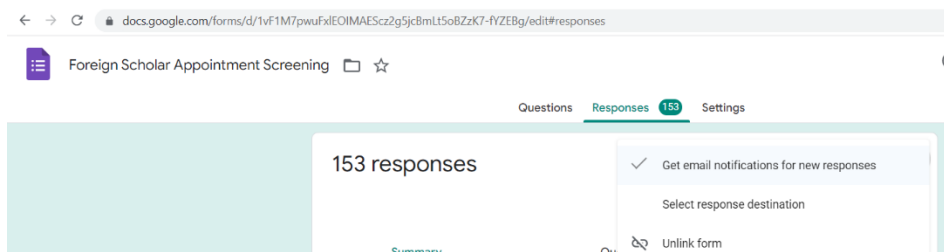
Foreign Scholar Screening Requests

1. The department or faculty requests a foreign scholar screening from RSO's website: https://research.umd.edu/resources/research-compliance/export-compliance-office-eco/foreign-scholar-appointments. The department or faculty submits the foreign scholar screening request on a Google Form. All foreign nationals who will have UMD appointments, whether staff, faculty, or students, are required to be screened by RSO. RSO screening is required for unpaid appointments. RSO does not screen students who are foreign nationals without appointments.

1. The screening request survey is available once the department or faculty submits it. You can ask the Google Form to send you an e-mail when a foreign scholar screening request is submitted by clicking the three dots in the upper righthand corner…

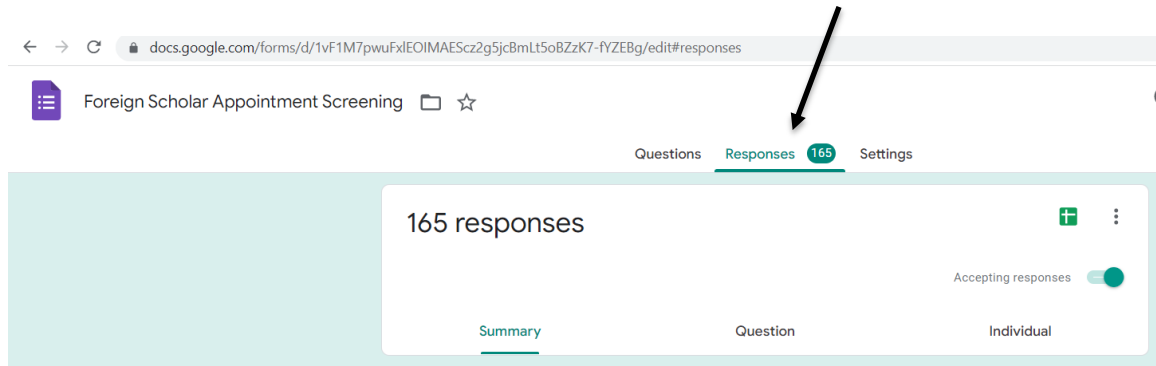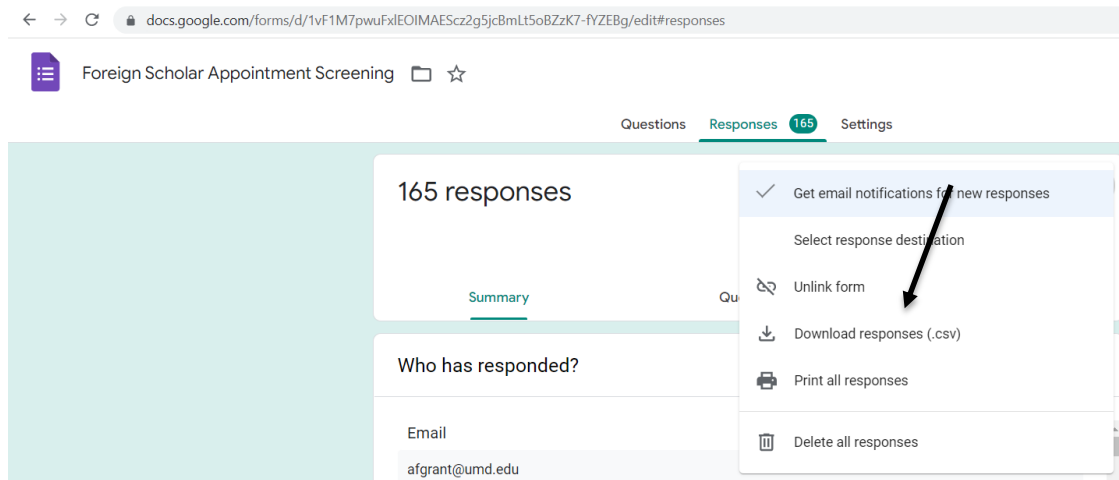…then choosing "Get email notifications for new responses."

2. Download the foreign scholar screening request. Open the Google Form, Foreign Scholar Appointment Screening. Choose Responses and click the three dots in the upper righthand corner…

...then choose Download Responses.

Open the downloaded file in Excel and find the foreign scholar screening request. You will need to manipulate the Excel file in order to prepare the foreign scholar screening request for review and approval. This includes wrapping the text in the headers and the submission, hiding other submissions, and printing the submission under review to pdf.

3. Screen the foreign scholar in [Visual Compliance](#).
   - Choose Restricted Party Screening.
   - Leave all defaults as-is.
   - Enter the foreign scholar's complete name and institution, if any, then click Screen. Ensure that any diacritics are correct. Visual Compliance can handle them, but Google sometimes alters them when the foreign scholar screening request is submitted.

For most foreign scholars, Visual Compliance will not find any matching records.

NO MATCHING RECORDS FOUND

If Visual Compliance does find a match for the individual or the institution, Visual Compliance will show which sources list the individual or institution.

For names that match, use common sense to determine whether any of the matches is actually the foreign scholar. For example, does the date of birth of the name in Visual Compliance match the date of birth on the foreign scholar screening request? If you cannot reasonably determine that the name in Visual Compliance is for someone other than the foreign scholar, route the foreign scholar screening request to the RSO Director for his review.

Reference	Name	FRC	Alert
REL026277	Drew SMITH TACOMA WA United States		Level 1

RPS Details

Reference No.	REL026277 Individual
Description	Drew SMITH 98406 TACOMA WA United States

For institutions that match, route the foreign scholar screening request to the RSO Director for his review.

Reference	Name	FRC	Alert
ELT058207	SICHUAN UNIVERSITY No. 24 South Section 1, Yihuan Road Chengdu	77 FR 58006	Level 1

RPS Details

Reference No.	ELT058207
Description	SICHUAN UNIVERSITY No. 24 South Section 1, Yihuan Road 610065 Chengdu 77 FR 58006 09/19/12 . For all items subject to thc EAR. Case-by-case basis.

Download the screening results as a pdf.

4. Read the foreign scholar screening request. If anything in the request needs further clarification, contact the person who submitted the request. Google Forms records the person's e-mail address when the request is submitted.
- The dates should make sense. The start date must be before the end date, and visas are not typically for longer than five years. Approximate dates are acceptable. A start date prior to submission of the foreign scholar screening request is not inherently problematic.
- The scope should describe in sufficient detail what the foreign scholar will be doing.
- If the foreign scholar has a paid appointment, check the funding source. A foreign scholar may be paid from more than one source.
    - If the foreign scholar will be paid from internal funds that is acceptable.
    - If the foreign scholar will be paid from a sponsored project, log into KR and read the award for any terms related to foreign national participation, whether the research is fundamental, and publication restrictions.
- The following foreign scholar screening requests must be routed to the RSO Director for approval after you complete initial due diligence research.
    - The foreign scholar is from a foreign government or a foreign military. Foreign public universities are not considered foreign government entities here.
    - A foreign military or a foreign for-profit is funding the foreign scholar.
    - The foreign scholar will be working on technology that may be used for defense purposes, per the scope.
    - The foreign scholar will be paid from a sponsored project that restricts foreign nationals.
    - The foreign scholar's faculty host has a TCP or RR waiver. The TCP log has a list of faculty with active TCP's. The TCP may be for a project other than the one funding the foreign scholar. The concern is separating the foreign national from the faculty host's restricted work.
    - The foreign scholar will be working on a project with a restricted research waiver. The RR waiver log has a list of faculty with active RR waivers. Read the RR waiver and its associated award to determine why the project has an RR waiver. See if the foreign scholar will be working on a thesis or dissertation that could be affected by the restrictions.
    - The foreign scholar screening request answer is yes to, "Will the foreign scholar have access to any proprietary or confidential technical information (other than information that will eventually be published), or have access to labs where developmental or export-controlled research is performed?" Before routing the request to the RSO Director for review, ask the person who submitted the request to confirm the answer is yes and to provide additional details.
    - The foreign scholar has an affiliate appointment, or has an appointment unfunded by either foreign sources or UMD.
    - The foreign scholar is a citizen of China, North Korea, Sudan, Syria, Russia, or Belarus.

5. To refer a foreign scholar screening request to the RSO Director for his review, send an e-mail with subject line, "***[DIRECTOR's NAME] PLEASE REVIEW*** Foreign Scholar Screening Request: [First Name] [Last Name]."

- Attach the screening results and the foreign scholar screening request to the e-mail.
- Describe why you are routing the request to the RSO Director, and attach any relevant documents, such as awards.

Add the foreign scholar screening request to the Status of Incoming ECO Requests log after routing the request to the RSO Director.

6. Once you are ready to approve the foreign scholar screening request, send the approval e-mail to the person who submitted the foreign scholar screening request. You must cc the RSO Director and the export reflector. In some departments, faculty submit the requests but department personnel should be cc'ed. The e-mail subject line should be "Foreign Scholar Screening Request: [First Name] [Last Name]."

This is the standard approval language.

> Good morning [Person who submitted the request],
>
> Please accept this email as confirmation that VPR has screened and cleared the subject individual for restricted party compliance purposes.
>
> **If the foreign scholar will be working or collaborating on any federally funded research, even if unfunded, the foreign scholar's support may need to be disclosed in proposals or active awards. Each funding agency has different disclosure and reporting requirements. Please** contact your ORA administrator **if you need to update disclosures on active awards.**
>
> The faculty host is responsible for contacting RSO if any information on the foreign scholar screening request changes so that RSO can re-screen the foreign scholar.
>
> This clearance does not confer any authorization to transfer export-controlled technology to the foreign scholar. Based on the answers you provided on the attached Foreign Scholar Screening Request form, it does not appear that an export license will be required to support the visit.
>
> If this person's visit requires an action in PHR, please use the date of screening as [MM/DD/YY].
>
> Thank you,
> [Your Name]

If the visitor is a citizen of Iran or Cuba, this is the standard approval language.

> Good morning [Person who submitted the request],
>
> *Due to the visitor's citizenship of a sanctioned country, this approval is subject to verification that the proposed activity is approved under the scope of the visitor's visa.*
>
> Please accept this email as confirmation that VPR has screened and cleared the subject individual for restricted party compliance purposes.

If the foreign scholar will be working or collaborating on any federally funded research, even if unfunded, the foreign scholar's support may need to be disclosed in proposals or active awards. Each funding agency has different disclosure and reporting requirements. Please contact your ORA administrator **if you need to update disclosures on active awards.**

The faculty host is responsible for contacting RSO if any information on the foreign scholar screening request changes so that RSO can re-screen the foreign scholar.

This clearance does not confer any authorization to transfer export-controlled technology to the foreign scholar. Based on the answers you provided on the attached Foreign Scholar Screening Request form, it does not appear that an export license will be required to support the visit.

If this person's visit requires an action in PHR, please use the date of screening as [MM/DD/YY].

Thank you,
[Your Name]

6. Save all documentation associated with the foreign scholar screening request to Box. Documentation must include the results of the Visual Compliance screening and the foreign scholar screening request. Also save any relevant correspondence. Save the documentation as a single pdf named "YYYY.MM.DD [Last Name]," with the Visual Compliance screening results first, then the foreign scholar screening request, then any relevant correspondence. One of the many reasons why saving documentation is crucial is that the State of Maryland requires UMD maintain records associated with each foreign scholar until five years after the end of the visit. Consistency in how foreign scholar screening requests are documented is also crucial given the volume of requests RSO receives.

7. Add the foreign scholar screening request to the log in Box.

Enter the answers to these questions in the "Any Foreign Funding Sources?" column in the log.

Will the visit be funded by any foreign sources of funding such as scholarships, salary, stipends, etc.? *

○ Yes

○ No

If you answered yes to the previous question, please describe foreign funding source(s) here:

Long answer text

Enter the answers to these questions in the "Paid or Unpaid Appt, and Account if Paid Appt?" column in the log.

Will the Foreign Visitor be a paid UMCP employee? *

○ Yes

○ No

If "Yes" to above, please list associated KFS number(s).

Short answer text

Enter the answers to these questions in the "Foreign Visitor's Scope of Work" column in the log.

Please describe the scope of the visiting scholar's activities at UMD: *

Long answer text

Please list any UMD projects the visitor will or may participate in including sponsored research, internal funding, gift-funded, or industry collaborations. (If none enter "none"): *

Long answer text

Outgoing Proprietary Technical Data

When researchers need to send proprietary technical data to a non-US individual (not a US citizen or Permanent Resident) or location, the transaction is considered a deemed export and treated by export regulations similarly to sending a physical item to the location for which the individual is a citizen. For certain technologies, an export license may be required in order to legally transmit the information. The

Research Security Officer is available to help make the licensing determination. Due to the long lead-time needed for obtaining export licenses, researchers are encouraged to contact the Research Security Officer as soon as they become aware of a potential need.

Physical Exports

When research equipment or specimens are sent out of the country, it is the responsibility of the shipper to verify whether there is an export licensing requirement for the particular item combined with its destination. This determination requires understanding whether the item is subject to ITAR or EAR jurisdiction by determining whether it is listed on the United States Munitions List (USML) (22 CFR Part 121) or the Commerce Control List (CCL)(15 CFR Part 774). Items not on either list are usually designated "EAR99" and can be shipped to most locations, excluding Iran, Syria, N. Korea, Cuba, Sudan, and other restricted entities, without a license. For items that are on the USML (military and space technologies) a license is generally required for every location outside of the US. Items on the CCL are designated with an Export Control Classification Number (ECCN) and have a licensing requirement for certain locations depending on the controls associated with the specific ECCN. There are also certain foreign entities including foreign academic institutions that are subject to special restrictions not otherwise applicable to their country. In addition to the licensing determination, the shipper is also responsible for complying with the Record Retention section herein.

Making the licensing determination requires significant expertise in the technology and export laws. Upon request, the Research Security Officer can assist departments in making these determinations which includes helping to assess the item's export jurisdiction and classification, screening foreign locations for restrictions, and making a licensing determination.

Departments that deal with a significant volume of international shipments of technology items may designate an Export Liaison.   The Research Security Officer provides annual training to the Export Liaisons on identifying shipments that may require a license.

The Research Security Officer is available to help make the licensing determination and assist with the export activity.   The process for initiating this review can be found on the Research Security Officer website at https://research.umd.edu/resources/research-compliance/export-compliance-office-eco/international-shipping. Due to the long lead-time needed for obtaining export licenses, researchers are encouraged to contact the Research Security Officer as soon as they become aware of a potential need.

Foreign Travel

When researchers travel to overseas locations, any accompanying equipment or technical data (stored on electronic devices or in hard copy) is considered by export laws to have been exported to their destination and any interim locations.   Certain countries also have sanctions programs administered by the Office of Foreign Assets Control which may prohibit travel activities, services, or other exchanges. Currently, Cuba, Syria, North Korea, Iran, and Sudan have the most restrictive sanctions impacting travel, shipment or carrying of items, and provision of services. Travelers are advised to contact the Research Security Officer prior to planning a trip to any of these locations. It is the responsibility of the traveler to understand any regulations that could impact their travel activities. The Research Security Officer is available to provide guidance to travelers as well as to help provide documentation to travelers exporting materials under an exemption.

The "International Travel" tab on the Research Security Officer website (https://research.umd.edu/research-resources/compliance/export-compliance-office-eco/international-travel) provides additional guidance on export compliance and travel as well as a form that can be utilized by travelers for temporarily carrying equipment to locations where it is necessary to have an export license or documented exemption (i.e. §740.9 Temporary imports, exports, reexports, and transfers (in-country) "TMP").

Record Retention

Export laws generally require the retention of all documents related to export activities for a period of 5 years from the activity date or date of expiration of an agreement. Documents requiring retention include but are not limited to: Agreements, awards, contracts, Technology Control Plans, export determinations, export transmittal records, exemption records, licenses, and shipping documentation.

The Office of Research Administration is responsible for maintaining all documentation related to sponsored research agreements in the COEUS system. The Research Security Officer is responsible for maintaining all documentation related to export determinations, trainings, Technology Control Plans, unfunded agreements, licensing, and exemptions. Faculty and Departmental Administrators are responsible for maintaining all records related to shipping documentation, export transactions, and exemption use resulting from activities under their control.

Reporting of Violations

Even when best efforts are employed to ensure compliance with export laws, there is always the potential for incidents to occur which may result in a violation of an

export law. An important aspect to this compliance plan is to identify potential violations early and take action to prevent recurrence. All parties have the responsibility to be vigilant and to report any potential issues to the Research Security Officer. When the Research Security Officer is notified, the Research Security Officer works with the Office of General Counsel to investigate the concern and make a determination, in coordination with the Vice President of Research, Export Compliance Committee, PI, Dean, Chair, Director, or Unit Head (as required), as to whether any remedial actions are necessary. Remedial actions could include creating or revising a Technology Control Plan, training, disciplinary actions, and/or reporting of the violation to the appropriate federal agency.

In the unlikely event that there is ever a suspected violation due to willful misconduct of an individual, the University has a Whistle Blower Protection Plan in place to protect the individual(s) reporting such behavior.   The plan can be found at the following site:

http://www.ora.umd.edu/sites/default/files/documents/news/guidance-umd-whistleblower-procedure.pdf

Although individuals are encouraged to make reports related to Export Compliance directly to the Research Security Officer, the program also includes a hotline for reports.

The program hotline is available at:
http://www.usmd.edu/usm/IAO/ReportFraud/index.php or 877-330-2320.