

University of Miami



Export Management & Compliance Program

Responsible University Officials: John L. Bixby, Ph.D.
Vice Provost for Research

William J. Collins
Export Control Compliance Director

Responsible Office: Office of Research Administration

Origination Date: July 21, 2017



Table of Contents

1. Program Statement5

2. Definitions5

3. Responsibilities5

 3.1. Export Control & Compliance Office6

 3.2. Empowered Official6

 3.3. Export Compliance Director (ECD).....6

 3.4. Leadership, Deans, Chairs & Department Administrators7

 3.5. Principal Investigators / Researchers7

 3.6. Employees8

 3.7. Students (Undergraduate, Graduate, Post-Doctoral, etc.).....9

 3.8. Visitors, Observers, Contractors.....9

4. Export Controls.....9

 4.1. Red Flags..... 10

 4.2. Export Control Reform Regulation Changes to Exports 10

 4.2.1. Exports: 10

 4.2.2. Deemed Exports: 10

 4.2.3. Foreign Person:..... 11

 4.3. Export Licenses 11

 4.4. Export Classifications..... 12

5. Biosafety..... 12

 5.1. Dual Use Research of Concern 13

 5.2. Working with Select Agents 14

 5.3. Importing / Exporting of Biological Materials 15

6. International Collaborations 16

 6.1. Research 16

 6.2. Study / Exchange Programs..... 18

7. Information Security..... 18

 7.1. Encryption..... 18

 7.2. Collaboration Tools..... 19

 7.3. Confidential Information 20



7.4.	Classified Research	21
7.5.	Unclassified Information	22
7.6.	Cloud Computing / Online Data Storage	22
7.7.	Laboratory Information Security	23
8.	Contracts and Awards	24
8.1.	Proposal Contract Routing Forms.....	24
8.2.	Restrictive Clauses	25
8.3.	NASA & China Affiliation.....	26
8.4.	Debarment / Restricted Persons	27
9.	Restricted Party Screening.....	28
9.1.	Authorized Users	28
9.2.	“Hits”	29
9.3.	USCIS I-129 Attestation	29
9.4.	Vendors.....	30
10.	Physical Security & Personnel Access.....	30
10.1.	Campus Access	30
10.2.	Foreign Persons	31
10.3.	Identification Badges	31
10.4.	Campus Tours / Visits	31
11.	Technology & Technical Data.....	32
11.1.	Purchase Requisitions.....	32
11.2.	Inventory & Tracking	33
11.3.	Shipping	33
12.	International Travel.....	34
12.1.	TMP License Exception	34
12.2.	License Exception BAG	35
12.3.	International SOS.....	35
12.4.	“Clean” Devices	35
13.	Reporting.....	36
13.1.	Recordkeeping.....	36
13.2.	Cane Watch	37



13.3.	Audits.....	37
14.	Training.....	37
14.1.	Export Compliance Basics.....	38
14.2.	Export Compliance for Researchers	38
14.3.	CITI Program	38
14.4.	Training Renewal	38
15.	Technology Control Plans	38
16.	Retention Policy	39
17.	Authorizing Signature.....	39
18.	Document Revision History	39
19.	Appendices	39



The University of Miami issued its policy on Export Compliance on February 1, 2014. This policy is located on UM's Export Control Compliance website (www.miami.edu/exportcontrol). All UM personnel should be familiar and understand the contents of this policy.

1. PROGRAM STATEMENT

The Export Control & Compliance program serves to assist the UM community in understanding U.S. export control laws and regulations that affect their UM business activities. To better assist UM personnel in navigating through the complexities of U.S. export control laws and regulations and the processes that need to be followed, the Export Management & Compliance Program (EMCP) has been created and will serve as a comprehensive manual to UM faculty and staff. If at any time you need guidance and/or assistance with anything mentioned in this document, please contact UM's [Export Compliance Office](#) (ECO).

Export control laws and regulations fall under the jurisdiction of three (3) primary regimes: The U.S. Department of State which oversees the International Traffic in Arms Regulations (ITAR), the U.S. Department of Commerce Bureau of Industry and Security which oversees the Export Administration Regulations (EAR), and the U.S. Department of Treasury Office of Foreign Assets Control (OFAC). Other federal agencies, such as the Food and Drug Administration (FDA) and the U.S. Department of Energy (DoE), also administer export control regulations that fall within its area of jurisdiction. However, for the purposes of this program, reference to U.S. export control laws and regulations will generally be those that fall under the ITAR, EAR or OFAC.

The EMCP will be reviewed every two years, or when significant changes to processes or policies occur.

2. DEFINITIONS

Please refer to UM's [Export Control Compliance website](#) for a list of acronyms and terms commonly found within U.S. export control laws and regulations, as well as UM's export compliance program.

"UM Personnel" refers to UM employees, faculty, students, trainees, visiting scientists, and other persons retained by or working at or for UM to conduct business.¹

3. RESPONSIBILITIES

All UM personnel retained by or working at or for UM must conduct their affairs in accordance with U.S. export control laws and regulations. UM personnel must be familiar with the U.S. export control laws and regulations, including important exclusions and exemptions, as they relate to their responsibilities.

All UM personnel is accountable for safeguarding the items identified as export controlled, confidential, restricted, proprietary or sensitive but unclassified (SBU). It is the individual responsibility of each person to be clear about all UM policies² and exercise reasonable care in using and sharing export controlled items and participating in activities where export controls apply.

All UM Personnel will ensure compliance with U.S. export control laws and regulations is achieved within their area of responsibility.

¹ Refer to [Export Compliance Policy EXPORT-P-002](#)

² Policies on or related to the same topic may be issued by multiple UM departments.



3.1. Export Control & Compliance Office

UM Export Control & Compliance office resides within the Office of Research Administration (ORA). The ECO is responsible for overall management of UM's export compliance program.

Export Control & Compliance
Office of Research Administration
Gables One Tower
1320 South Dixie Highway
Suite 650,
Miami, FL 33146

Office Phone: 305-284-9558
Website: <http://www.miami.edu/exportcontrol>
e-Mail: exportcontrol@med.miami.edu

3.2. Empowered Official

Barbara A. Cole of the Office of Research Administration (ORA) maintains the position as UM's Empowered Official (EO) for export compliance matters under the U.S. Arms Export Control Act³ and its regulations, and in this capacity has the authority to:

- (a) Oversee all UM export licensing or approval activities, including signing license applications or other documentation relating to such licensing or exporting approval.
- (b) Approve any and all written exceptions to export control requirements.
- (c) Represent UM before export control regulators in matters related to registration, licensing, commodity jurisdiction and classification requests and voluntary disclosures.
- (d) Bind UM in any proceeding before any government agency with export control responsibilities.

Under regulation 22 CFR §120.25 the EO is the U.S. person who is directly employed by the Institute or a subsidiary; is legally empowered in writing to sign license applications or other requests for export approval; understands the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability, and administrative penalties for violating the regulations; and has the independent authority to:

- (e) Inquire into any aspect of a proposed export, temporary import, or any other transaction within the scope of export control regulations.
- (f) Verify the legality of the transaction and the accuracy of any information to be submitted to a licensing or approval authority.
- (g) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse being taken by the Institute.

As implied by 22 CFR §120.25, the EO is free of any encumbrances and operates under the full support of UM's administration to pursue without interference for any and all forms of investigation required to comply with all export control laws and regulations as well as UM's Export Management & Compliance Policy (EMCP).

3.3. Export Compliance Director (ECD)

The ECD reports to ORA and undertakes responsibilities such as the following:

- (a) Monitors export control developments (legislation, regulations, cases, penalties, etc.) and develops procedures to ensure UM remains in compliance with all export control regulations (not limited to the EAR, ITAR, and OFAC).
- (b) Identifies UM activities that are or may be impacted by export control regulations and develops strategies and procedures to manage the risks.
- (c) Recommends procedures to the senior UM administration to maintain UM's compliance.
- (d) Works with all personnel on all campuses to facilitate understanding and compliance with export control related matters.
- (e) Assists investigators, researchers and offices within UM when research or research results are export controlled.

³ 22 USC §2778



- (f) Assists researchers in understanding export control issues related to their research activities, data, software, and technology transfer, so they may be in compliance with export control regulations.
- (g) Develops a Technology Control Plan (TCP) for each export-controlled project consistent with this EMCP to aid the principal investigator (PI) in meeting his/her export control responsibilities.
- (h) Applies for export licenses, Commodity Jurisdictions (CJ), Export Control Classification Numbers (ECCN), Technical Assistance Agreements (TAA), and Technology, Hardware and Software licenses and the utilization of license exemptions and exceptions including other export approvals.
- (i) Advises and approves, with regard to export control issues, all foreign persons visiting UM under visa sponsorship.
- (j) Investigates and documents voluntary disclosures of any violations of the export control laws and regulations.
- (k) Serves as administrator for the Restricted Party Screening (RPS) tool.

The ECD may also be designated, by the ORA in writing, as an Empowered Official with the additional authority defined in Section 3.2 above.

While certain oversight functions may be delegated, only an EO has the power to sign paperwork which binds UM in any proceeding before the DDTTC, BIS, OFAC, or other government agency with export control responsibilities⁴.

All communications with U.S. licensing authorities shall be made only through the Export Compliance Officer or the Vice Provost for Research.

3.4. Leadership, Deans, Chairs & Department Administrators

Leadership, Deans, Chairs and Department Administrators shall extend their commitment to UMs overall success by including support of the export compliance program. Responsibilities shall include, but not be limited to:

- (a) Familiarization with export compliance management and compliance requirements, including those presented in this EMCP.
- (b) Dissemination of Export Control & Technology Management policies, processes and communiqué throughout their areas of responsibility.
- (c) Active participation in export compliance training.
- (d) Sharing responsibility for developing procedures and training programs that include compliance with export control laws and regulations.
- (e) Linking to corresponding policies, processes and training programs in other administrative units.
- (f) Identification of students and faculty from foreign countries by program/department and taking appropriate steps outlined by UM policy.

3.5. Principal Investigators / Researchers

UM Principal Investigators (PI's) and researchers are central to export control management and compliance. They work with strategically important technologies, engage foreign persons in their laboratories, and advise them on their studies. They participate in international research collaborations, conferences, and scientific and technical exchanges in the U.S. and abroad; host campus visitors; and engage in other activities that may be subject to export controls.

PIs with the assistance of the ECO, Office of Research Administration (ORA), and other relevant UM departments, are responsible for full compliance with all federal and UM export compliance requirements in the conduct of their research. To meet these obligations, each PI must:

- (a) Understand the export compliance obligations and participate in regular trainings to be able to identify export control issues;
- (b) Be aware of export control indicators and note such information on any internal compliance or assurance forms;
- (c) Confirm, **prior to initiation of research or international travel**, whether any information or technology involved is subject to trade sanctions;

⁴ [22 CFR §120.25](#)



- (d) Periodically review scope of project, processes and records to ensure continuing compliance with export control laws and regulations;
- (e) Briefing all research personnel involved in the project of their export compliance obligations; and
- (f) Understand that any informal agreements or understandings entered into with a sponsor may negate the Fundamental Research Exclusion (FRE) or other key exclusions and impose export control obligations on the PI and the research team.

While the procedures outlined in this EMCP will assign specific responsibilities, it is essential that all researchers and staff, and especially PIs:

- (a) Become familiar with export controls and compliance, using communications and training provided by the Export Control & Technology Management Office. It is not necessary to become experts, but **researchers are expected to develop a basic understanding so as to know when to raise questions and alert UM to possible export control issues.**
- (b) When possible, refrain from entering into any agreement applicable to their research or UM employment that defeats the FRE⁵. This includes language **restricting participation of foreign persons, sponsor approval of publications, non-disclosure agreements, confidentiality agreements, and 'side bar' agreements** related to UM research.⁶
- (c) Evaluate research opportunity at the **earliest stage** (i.e., proposal stage) to identify possible export control issues (especially the use of development of strategic technologies, and involvements of foreign persons as students, staff, and collaborators), flag these issues, and discuss them **prior** to making a proposal or any other commitment to do the work.
- (d) Once the project has begun, re-evaluate export control decisions as a result of changes in project scope, staffing, use of export-controlled items provided by third parties, and any other changes in project circumstances.
- (e) Consult with the ECO in a timely fashion to permit the time needed to evaluate the research in question and obtain any necessary licenses or authorizations. (Refer to [Section 4.3](#))
- (f) Refrain from bringing any item (commodity, technical data, or technology) or a proprietary software package obtained as part of an outside consulting assignment onto the campus or into a UM research project that is not already part of campus research or educational activities, and that may be subject research or educational activity to export controls.
- (g) Contact the ECO when there is a high probability that an item will be used directly or indirectly in activities related to satellites, missiles, chemical/biological weapons, or sensitive nuclear activities.
- (h) Coordinate with the recipient of all materials to make sure that he/she has obtained the proper importation permits.
- (i) Ensure that all items sent to foreign persons, foreign entities, or foreign countries are packaged according to applicable U.S. Customs and export regulations.
- (j) Identify laboratories and/or specialized equipment that could be subject to export control laws and regulations.
- (k) Disseminate of export compliance policies, processes and communiqué throughout their areas of responsibility.
- (l) Monitor and document activities for compliance.
- (m) Self-report for non-compliance activities.
- (n) Actively participate in export compliance training sessions and renew training as required.

3.6. Employees

It is the individual responsibility of each UM personnel to secure their research and technology, chemicals and biological materials that they handle, and proprietary and Government articles or information entrusted against unauthorized use or theft.

UM personnel are responsible for ensuring foreign persons, visitors, observers, outside vendors, etc., have all been screened to confirm that the person or entity does not appear on any of the 200+ agency lists of denied/excluded parties. (see [section 9](#) and [section 10](#) for more details)

⁵ PIs who are working on patentable technology do not qualify under the FRE and thus may include restrictive clauses in order to protect the innovation.

⁶ PIs should work with ORA and / or General Counsel to review language and negotiate restrictions that all parties can comply with.



UM personnel who seek to export an item shall be responsible for performing the export licensing analysis for any potential export. Various checklists and decision trees are located in the [appendix](#) of this document to assist UM personnel in determining if export controls may apply to the particular circumstances at hand. UM personnel should also consult with the UM's ECO for additional guidance.

3.7. Students (Undergraduate, Graduate, Post-Doctoral, etc.)

It is the responsibility of each UM student to secure their research and technology, chemicals and biological materials that they handle, and proprietary and Government articles or information entrusted against unauthorized use or theft.

All students assigned to work on research which involves export-controlled technology and/or technical data are required to attend export compliance training conducted by UM's ECO. This training is required before work on any project with such items commences and will be arranged by the PI. Students understand that assignments involving export-controlled technology may be restricted from inclusion in academic requirements such as dissertation or thesis.

3.8. Visitors, Observers, Contractors

All official visitors coming to UM for official business or educational purposes must be invited by authorized UM personnel within a UM unit that has recognized authority to oversee the activity the respective visitor is present for.

Frequent visitors, such as contractors, observers, or volunteers who are engaged in long-term UM sanctioned activities may be required to obtain a UM ID / badge as deemed appropriate by the UM unit with recognized authority to oversee the activity. IDs / Badges are issued by each respective campus access control authority.

Any person who has a UM ID / badge may only enter the access-controlled areas that they have access-rights/permissions to enter. To enter any other area, the person must be authorized and escorted at all times by authorized UM personnel with access permission for the area.

4. EXPORT CONTROLS

U.S. export control laws and regulations have been in force since the 1940's. It has only been since the terrorist attack of September 11, 2001 on U.S. soil that enforcement of these laws and regulations has been heightened, especially at institutions of higher learning and research. These laws and regulations affect many facets of business whether activities take place on U.S. soil, in International Waters, air space or foreign land. The technology used within business today, especially with respect to personal computers, only adds to the complexities of how and when export control laws and regulations are applicable especially as it pertains to research collaborations with foreign persons.

In 2009, the Export Control Reform (ECR) initiative began with reorganizing and streamlining the U.S. export control regimes in the U.S. Department of Commerce's Bureau of Industry and Security (BIS), which oversees the Export Administration Regulations (EAR) and the Department of State's Directorate of Defense Trade Controls (DDTC) that has jurisdiction of the International Traffic in Arms Regulations (ITAR).

The ECR reduced regulatory burdens on U.S. companies and institutions of high learning and research while increasing the effectiveness of controls on the most sensitive defense-related goods and technologies. Placing a higher fence around fewer items in the ITAR and EAR. ECR-related BIS and DDTC rule changes focused on transferring certain goods and technology from the ITAR-U.S. Munitions List (USML) to the EAR-Commerce Control List (CCL), or deregulating them altogether.





Understanding when and how export controls apply to a particular item or situation is not always black and white. All facets must be examined in order to make the proper conclusion and determine correctly whether or not export control laws and regulations apply. Because the regulations are in flux, the decision made 6 months ago may not apply today to a similar situation. Re-examining the facets feeding into the situation, regardless of how minor they may seem or irrelevant to the situation, is essential. **Assumptions are not an option in determining export control applicability.**

4.1. Red Flags

The following are indicators that an export control review should be conducted to ensure that no violations will occur. See also [Appendix B](#) for more indicators⁷.

- (a) The results of the research conducted at UM or by UM personnel are intended for military purposes or for other restricted end-uses.
- (b) Foreign persons will have access to controlled items.
- (c) Software which include encryption features are being developed or purchased.
- (d) UM faculty or staff who will export or travel abroad with research equipment, chemicals, biological materials, encrypted software, non-public source code, or other controlled items; or travel abroad with laptops, cell phones, PDAs, or tablets containing controlled information or encryption software. This also includes conducting research in international / foreign waters with such items.
- (e) Any proposed transaction that will involve embargoed countries or entities, individuals located in embargoed countries, or individuals who are on prohibited or restricted end-user lists as determined through RPS.
- (f) The sponsor requires pre-approval rights over publications or the participation of foreign persons.
- (g) The sponsor excludes the participation of foreign persons.
- (h) The project requires the shipping of equipment to a foreign country.
- (i) The project requires deployment/retrieval and other research activities in International Waters.
- (j) Collaborations with foreign governments⁸, foreign government officials, or collaborations with individuals or entities of embargoed countries.⁹

4.2. Export Control Reform Regulation Changes to Exports

Export Control Reform initiatives furnished important changes and clarifications to the definitions of "export," "deemed export", "foreign person", "reexport," "transfer," "technology" and "fundamental research" that will be of particular interest to industry and research institutions, including universities. This section will discuss the following "exports", "deemed exports" and "foreign persons".

4.2.1. Exports:

An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner¹⁰. Exporting can also include verbal or written transmissions or communications (phone calls or emails) with persons located in other countries, even if the recipient is a U.S. person or transmission or communications carried out in the United States, if the recipient is a foreign person.

4.2.2. Deemed Exports:

A "deemed export" occurs when there is a "release in the United States of 'technology' or source code to a foreign person." Similarly, "release" is defined in the BIS Rules as "visual or other inspection by a foreign person of items that reveals 'technology' or source code subject to the EAR

⁷ The list is not all inclusive and is only to serve as a guide.

⁸ UM personnel should take caution when engaging in activities with foreign governments and/or foreign government officials in that violation of the Foreign Corrupt Practices Act (FCPA) do not occur.

⁹ Embargoed countries include: Cuba, Syria, Sudan, Iran, and North Korea. Certain embargoes are still in effect with China. This list can change at any given moment, thus UM personnel should consult with the ECO in advance.

¹⁰ Export Administration Regulations. [15 CFR 734.13](#)



to a foreign person."¹¹ This adheres to long-standing BIS policy, **the requirement that such inspection must "reveal" makes it explicit that a foreign person merely seeing an item or "having theoretical or potential access" to technology or software is not sufficient to constitute a deemed export.**¹² Technology is "released" for export when it is available to foreign persons for visual inspection (such as reading technical specifications, plans, blueprints, formulae, source code, object code, etc.); when technology is exchanged orally; or when technology is made available by practice or application under the guidance of persons with knowledge of the technology.¹³ Example: The transfer of infrared camera technology to a Chinese national in the U.S. may be regulated as if the transfer of the technology was made to the Chinese national in China. The transfer is thus "deemed" to be to China even though all activities take place in the U.S.

4.2.3. Foreign Person:

A foreign person is a person who has been granted access into the United States on a visa. Persons who have been granted permanent residence (green card), U.S. citizenship, or are considered protected¹⁴ are not considered foreign nationals¹⁵. BIS Rules simplified the terms used in the EAR to designate non-U.S. persons by adopting the ITAR nomenclature of "foreign person" instead of "foreign national."

4.3. Export Licenses

UM's ECO will establish which license type is appropriate from the U.S. Department of State (USDOS) and the U.S. Department of Commerce (USDOC). Items that have been determined to require an export license cannot be exported or released until the export license has been received in-hand by UM's ECO and reviewed with the Principal Investigator (PI) or department administrator. Only UM's ECO is able to submit license applications on behalf of UM, and only the EO will have signing authority.

The time it takes to obtain an export license varies. Some cases have taken as little as 6 weeks whereas others have taken as much as 6 months or more. Providing detailed information and supporting documentation, even if not required for the license, may help in reducing the application review time by the U.S. Government.

Supporting documentation required for a license application may include, but is not limited to:

- Technology Control Plan
- Product Spec Sheets
- Floor Plans
- Diagrams, Formulae, Blueprints, and other related technical data
- Statement of Work
- Executed Agreement / Contract
- Resume / Curriculum Vitae for each project staff member (compensated or not)
- Job Description for each project staff member (compensated or not)
- Export Classification Certification form (EXPORT-F-002) from vendor/manufacturer
- Restricted Party Screening verification
- Shippers Export Declaration or Automated Export System (AES) record

ORA's ECO conducts a complete analysis and an inter-organizational review of the UM license application along with all documentation to be submitted in support of the application to the Department of Commerce and to the Department of State.

A Team consisting of the ECO and ORA Senior Contracts specialists, review license applications to ensure:

- proper licensing jurisdiction either in the EAR or ITAR
- ECCN and Category of the item

¹¹ Export Administration Regulations. [15 CFR 734.15](#)

¹² [81 Fed. Reg. 35586, 35592](#)

¹³ [Export administration Regulations 15 CFR 734.15\(a\)\(1\)\(2\)](#)

¹⁴ [8 U.S.C. 1324b\(a\)\(3\)](#)

¹⁵ There may be some situations where nationality takes precedence and those who are U.S. Permanent Residents may be restricted from certain activities.



- its destination
- prohibited end use
- end user verification – Restricted Party Screening (RPS)
- review license exceptions and exemptions
- Statement of Work
- Attachments

4.4. Export Classifications

All items have an export classification. Identifying the export classification is essential in understanding the restrictions to foreign persons and exporting overseas. Classifications will either be a 5-digit alpha-numeric sequence or Roman numeral. UM is not in a position to understand the technical assessment of the item or the original design intent (ODI) in order to determine the correct export classification. Per [15 CFR 758.3](#), the vendor or manufacturer is to supply this information upon request. The classification of items is to be declared using form [EXPORT-F-002](#).

Commercial / Dual-Use items will fall under the jurisdiction of the BIS and will be assigned an export control classification number (ECCN) that is characterized by an alpha-numeric sequence, example: 1A001, 4B994, 7D994, and appear on the Commerce Control List (CCL). Items that are not specifically identified on the CCL will be assigned a classification of “EAR99” which serves as a “basket” designation. Items that are identified as “EAR99” can be exported / released to **most** destinations under **most** circumstances, but may be restricted to foreign persons and countries that appear on the U.S. Department of State list of embargoed countries.

Military items will fall under the jurisdiction of the Department of State and will be assigned a classification that is characterized by a Roman numeral, example: VII(h), XI(d), and appear on the U.S. Munitions List (USML). Any item appearing on the USML will require authorization from the U.S. Government in the form of an export license before the item can be released to any foreign person regardless of location, or exported outside of the United States including into International Waters.

It is perfectly acceptable to ask the vendor/manufacturer for the export classification number of any item you want to procure at the time of quoting. Obtaining this information in advance of submitting the purchase requisition through UM Purchasing will help expedite the export compliance review process and approval flow.

5. BIOSAFETY

The safe handling and disposal of hazardous biological materials is an integral component of the Laboratory Safety Program at UM. Hazardous biological materials include bacteria, viral agents, fungi, and protozoans, plus agents produced by means such as recombinant DNA technology. Part of the risk to laboratory workers from these agents stems from the fact that they are invisible to the naked eye and hence their presence may be undetected. Another risk is their potentially contagious nature, allowing them to spread from person to person. Thus an infection acquired in the laboratory could be disseminated far from its original source.

All PIs and research staff who work with biological agents are to be familiar with UM's [Environmental Health & Safety policies and processes](#). The Biological Safety Program assists PIs and research staff in implementing all applicable regulations, standards and guidelines when handling infectious or potentially infectious biological agents in research and clinical laboratory and other facilities.

If you work or intend to work in recombinant DNA research, you must comply with the National Institute of Health (NIH) Guidelines for Research Involving Recombinant DNA. Compliance with the NIH Guidelines requires the PI to make the appropriate biological risk assessment of his/her rDNA construct and to assign the appropriate Risk group. To get approval to do rDNA research at UM, the PI is to contact the Institutional Biosafety Committee (IBC).¹⁶

¹⁶ Institutional Biosafety Committee (IBC) –<http://uresearch.miami.edu/regulatory-compliance-services/ibc> or phone (305) 243-2311



5.1. Dual Use Research of Concern

September 24, 2014, the United States Government released the United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern¹⁷. The policy addresses institutional oversight of DURC, which includes policies, practices, and procedures to ensure DURC is identified and risk mitigation measures are implemented, where applicable. Institutional oversight of DURC is the critical component of a comprehensive oversight system because institutions are most familiar with the life sciences research conducted in their facilities and are in the best position to promote and strengthen the responsible conduct and communication¹⁸. This policy and the March 2012 DURC Policy released March 29, 2012¹⁹ and updated in February 2013²⁰ are complementary and emphasize a culture of responsibility by reminding all involved parties of the shared duty to uphold the integrity of science and prevent its misuse. The new policy applies to all federal agencies, as well as institutions that receive federal funding or that are conducting research that meets the definition of dual use research of concern (DURC), regardless of funding source. The new policy limits the scope of DURC to fifteen (15) Select Agents / Toxins²¹ and seven (7) categories of experiments. Non-compliance with the policy could result in the loss of federal funding for the institution.

Life sciences research that uses one or more of the agents or toxins listed below and produces, aims to produce, or can be reasonably anticipated to produce one or more of the effects listed will be evaluated for DURC potential.

Agents & Toxins	
Avian influenza virus (highly pathogenic)	Marburg virus
Bacillus anthracis	Reconstructed 1918 influenza virus
Botulinum neurotoxin	Rinderpest virus
Burkholderia mallei	Toxin-producing strains of Clostridium botulinum
Burkholderia pseudomallei	Variola major virus
Ebola virus	Variola minor virus
Foot-and-Mouth Disease virus	Yersinia pestis
Francisella tularensis	

Categories of Experiments (Effects)	
<ul style="list-style-type: none"> ○ Enhances the harmful consequences of the agent or toxin. ○ Disrupts immunity or the effectiveness of an immunization against the agent or toxin without clinical and/or agricultural justification. ○ Confers to the agent or toxin resistance to clinically and/or agriculturally useful prophylactic or therapeutic interventions against that agent or toxin or facilitates their ability to evade detection methodologies. ○ Increases the stability, transmissibility, or the ability to disseminate the agent or toxin. 	<ul style="list-style-type: none"> ○ Alters the host range or tropism of the agent or toxin. ○ Enhances the susceptibility of a host population to the agent or toxin. ○ Generates or reconstitutes an eradicated or extinct agent or toxin listed above.

¹⁷ US Government Policy update released 09/24/2014 (<https://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf>)

¹⁸ US Government Policy – U.S. Department of Health & Human Services (<https://www.phe.gov/s3/dualuse/Pages/InstitutionalOversight.aspx>)

¹⁹ US Government Policy released 03/29/2012 (<http://www.phe.gov/s3/dualuse/Documents/us-policy-durc-032812.pdf>)

²⁰ DURC Policy released 02/2013 (<http://www.phe.gov/s3/dualuse/Documents/oversight-durc.pdf>)

²¹ These agents and toxins are regulated by the Select Agent Program under Federal Law (7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73)



5.2. Working with Select Agents

All PIs and research personnel are to be familiar with "[EHS Laboratory Safety Manual](#)". This document defines UM's policy and processes to comply with the additional requirements for transferring or receiving select agents under U.S. laws and regulations.²²

Both the EAR and the ITAR²³ have provisions for the control of pathogens and toxins. The control level is different depending on which regulations control the items. Title 42 of the Code of Federal Regulations Part 73 covers "Possession, Use, and Transfer of Select Agents and Toxins."²⁴ The biological agents and toxins listed below have the potential to pose a severe threat to public health and safety. Tier 1 select agents and toxins (noted by an asterisk*) are subject to additional Health & Human Services (HHS) requirements that are outlined in the regulations.

Abrin
Botulinum neurotoxins*
Botulinum neurotoxin producing species of
*Clostridium**
Conotoxins
(Short, paralytic alpha conotoxins containing the following amino acid
sequence X₁ CCX₂ PACGX₃ X₄ X₅ X₆ CX₇)
Coxiella Burnetii
Crimean-Congo haemorrhagic fever virus
Diacetoxyscirpenol
Eastern Equine Encephalitis virus
Ebola virus*
Francisella tularensis*
Lassa fever virus
Lujo virus
Marburg virus*
Monkeypox virus
Reconstructed 1918 influenza virus (Reconstructed
replication competent forms of the 1918 pandemic influenza virus
containing *any* portion of the coding regions of *all* eight gene
segments)
Ricin
Rickettsia prowazekii
SARS-associated coronavirus (SARS-CoV)
Saxitoxin
South American Haemorrhagic Fever viruses:
 Chapare
 Guanarito Junin
 Machupo
 Sabia
Staphylococcal enterotoxins (subtypes A-E)
T-2 toxin
Tetrodotoxin
Tick-borne encephalitis virus
Far Eastern subtype
Kyasanur Forest disease virus
Omsk haemorrhagic fever virus
Variola major virus (Smallpox virus)*
Variola minor virus (Alastrim)*
Yersinia pestis*

²² 43 CFR §73, 7 CFR Part 331, 9 CFR Part 121 and the USA Patriot Act (PL 107-56).

²³ See Category XIV of the USML, TOXICOLOGICAL AGENTS, INCLUDING CHEMICAL AGENTS, BIOLOGICAL AGENTS, AND ASSOCIATED EQUIPMENT.

²⁴ 42 CFR Part 73 (http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title42/42cfr73_main_02.tpl)



The aggregate amount of toxin under the control of the PI, treating physician or veterinarian, or commercial manufacturer or distributor do not require an export license provided they do not exceed the amounts noted below:

Abrin	100 mg
Botulinum neurotoxins*	0.5 mg
Conotoxins (Short, paralytic alpha conotoxins containing the following amino acid sequence X ₁ CCX ₂ PACGX ₃ X ₄ X ₅ X ₆ CX ₇)	100 mg
Diacetoxyscirpenol	1,000 mg
Ricin	100 mg
Saxitoxin	100 mg
Staphylococcal enterotoxins (subtypes A-E)	5 mg
T-2 toxin	1,000 mg
Tetrodotoxin	100 mg

All select agents and toxins noted in [42 CFR §73.3\(b\)](#) will require authorization from the U.S. Government. [42 CFR §73.3\(d\)](#) will note the criteria that HHS select agents or toxins must meet in order to be excluded from the requirement of this part. **ALL** biological agents and toxins, regardless of amounts, **MUST** be registered with UM's Environmental Health & Safety office²⁵ **BEFORE** such agents and toxins are brought onto UM property.²⁶ The PI is to contact the Bio & Lab Safety Manager directly.

The Center for Disease Control (CDC) and the U.S. Department of Agriculture (USDA) - Animal and Plant Health Inspection Service (APHIS) share responsibility for some agents because they potentially threaten both humans and animals (overlapping agents). The laws require the Department of Health and Human Services (HHS) and USDA to review and republish the lists of Select Agents and toxins on at least a biennial basis (every 2 years). Therefore, it would behoove the PI or responsible administration office to review the Select Agents and Toxins page on the National Select Agent Registry website²⁷ on a regular basis for updates.

5.3. Importing / Exporting of Biological Materials

Any shipment of Dangerous Goods, Hazardous Materials, Biological Products, Infectious Substances or Diagnostic Specimens must comply with the International Air Transportation Association (IATA) Dangerous Goods regulations and the U.S. Department of Transportation regulations on Shipment of Hazardous Materials²⁸ and is coordinated through UM's Office of Environmental Health and Safety (EHS).²⁹ Prior to shipping or being involved in the process of shipping any dangerous goods or hazardous materials, any person at UM must receive training offered by EHS. Upon successful completion of the training, EHS will issue a certificate of attendance which is valid for two years from the date of issuance to the respective employee.

Importing and Exporting of export-controlled agents and toxins will be handled through EHS who will collaborate with the ECO to obtain the necessary Government authorization required.

The governing United States Agency for exporting and importing Biological products is the U.S. Food & Drug Administration (FDA). Within the FDA, the Center for Biologics Evaluation and Research (CBER) regulates biological and related products, including blood and blood products (which includes certain kinds of devices), vaccines, allergenics, tissues, and cellular and gene therapies. CBER also regulates the medical devices involved in the collection, processing, testing, manufacture and administration of licensed blood, blood components and cellular products and all HIV test kits used both to screen donor blood, blood components, and cellular products and to diagnose, treat, and monitor persons with HIV and AIDs. In order to import a CBER-regulated product into the United States, the product must meet FDA's regulatory requirements. The Division of Case Management (DCM) within CBER's Office of Compliance and Biologics Quality (OCBQ) directs and coordinates CBER's import program.

²⁵ Environmental Health & Safety website (<http://business-services.miami.edu/departments/ehs/index.html>)

²⁶ EHS Policy BSD-140 (<https://umshare.miami.edu/web/wda/policiesprocedures/Environmental/PDF-VERSION/BSD-140.pdf>)

²⁷ National Select Agent Registry (<https://www.selectagents.gov/SelectAgentsandToxins.html>)

²⁸ [49 CFR 100-185](#)

²⁹ Reference [EHS Policy BSD-035](#) or <http://business-services.miami.edu/about/index.html>



Please visit the FDA web site for more details:

<https://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/ComplianceActivities/BiologicsImportingExporting/ucm143371.htm>

Records of shipments of dangerous goods shall be maintained by the department of office originating the shipment in electronic or hard copy format and kept for not less than a year from the actual day of shipment. If the shipment involves export controlled agents or toxins, records must be maintained per [section 16](#) of this policy.

6. INTERNATIONAL COLLABORATIONS

All UM offices and departments are responsible for developing and implementing policies and procedures that align with the EMCP, when appropriate. It is the individual responsibility of each UM office and department to seek and obtain appropriate export compliance approvals from the ECO for international collaboration, research or other activities that take place outside of the United States.

All foreign person faculty and scholars teaching, conducting research, or presenting workshops, symposia, or other academic presentations who are not employed by UM must undergo RPS prior to participation in any academic or research programs. Failure to screen such persons in advance could result in freezing of compensation requests to such persons.³⁰ Requests for RPS screening are to be submitted on [EXPORT-F-006](#). See [Appendix I](#) for “Export Compliance Decision Tree for International Visitors” for additional guidance.

Departments who sponsor a visiting scholar will be responsible for screening such persons through UM’s RPS system **before** extending the invitation or offer letter. Requests can be submitted on EXPORT-F-006. The UM department who invite / host J-1 scholars and international observers will be required to include a copy of the approved screening results along with other applicable documentation defined in the Observership or Exchange Visitor Program Policies and Procedures.³¹

6.1. Research

Data and information involved in university research can be excluded from export control regulations under the EAR or ITAR **if** it meets all criteria for one of several key provisions: (a) the Public Domain Exclusion (PDE); (b) the Fundamental Research Exclusion (FRE); and (c) the Exclusion for Educational Information (EEI).

1. **Public Domain Exclusion (Publicly Available):** Information and items in the public domain, as that term is defined in 15 CFR §734.3(b)(2)(3) under the EAR; 22 CFR §120.11 under the ITAR, are not subject to control under those regulations.
 - a. Under the EAR, “publicly available” means:
 - i. Printed and published materials, prerecorded phonographic records, exposed or developed microfilm, motion picture film and soundtracks, reproducing printed and published content; or
 - ii. Public release of controlled technical data “in any form” (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency; or
 - iii. Fundamental research
2. **Fundamental Research Exclusion (FRE):** The FRE, as set forth in both the EAR and ITAR, is pursuant to an Executive Order issued by President Reagan in 1985 and still in effect today (NSDD 189). This Order requires that: “to the maximum extent possible, the products of fundamental research remain unrestricted.” The Order also directs that national security interests be protected through National Security Classification, not by restricting the conduct or reporting of unclassified research.

³⁰ Payments to foreign persons who are on a denied/restricted party list are a violation of OFAC regulations.

³¹ Exchange Visitor Program document is owned by International Student and Scholar Services (ISSS). Observer-ship program document is owned by The Harrington Group. Departments should review the policies and forms owned by ISSS and The Harrington Group.



Pursuant to this Order, both the EAR and the ITAR exclude fundamental research from export controls. Generally speaking, the FRE applies only to information and technical data, and not to controlled physical items.

- a. Under the EAR due to the ECR, Fundamental research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons³².
- b. The revisions of "fundamental research" moved away from the former definition's focus on the locus of research (e.g., whether it is conducted at a university, private industry or for the federal government), and instead provides a more precise definition of the term that closely tracks the definition currently used in the current ITAR³³. Therefore, the location in which fundamental research takes place does not matter so long as the definitional requirements of fundamental research are met.
- c. Also modified under ECR, the provision which excludes technology and software that "arises during, or results" from "fundamental research" from export control restrictions³⁴.
- d. Additionally, the new definition does not include any reference to research being "basic" or "applied," which BIS did not view as providing any additional clarity.
- e. Furthermore, BIS reiterated that **commodities** resulting from fundamental research are not excluded from EAR restrictions; the fundamental research exclusion applies only to software and technology.

University research is **NOT** considered fundamental and thus subject to the EAR if:

- i. Publication of research results is subject to restriction or withholding of research results, or substantial prepublication review, by a sponsor (other than for the protection of patents and/or sponsor's confidential proprietary information); or
 - ii. The research is funded by the U.S. Government and is subject to specific access and dissemination controls; or review of research within "any appropriate system" to "control the release of information" pertaining to research performed for a federal agency or a Federally Funded Research and Development Center (FFRDC); and
 - iii. Inputs used for fundamental research (which includes information, software and equipment) that are themselves not intended to be published are also not eligible for the fundamental research exclusion³⁵.
- f. Similarly, under the ITAR, fundamental research means basic and applied research in science and engineering at an accredited institution of higher learning in the United States, where the resulting information is ordinarily published and shared broadly in the scientific community.

University research is **NOT** considered fundamental and thus is subject to the ITAR if:

- i. Publication of scientific and technical information resulting from the activity is restricted; or
- ii. The research is funded by the U.S. Government and is subject to specific access and dissemination controls.

3. **Exclusion for Educational Information**: The ITAR specifically excludes from regulation information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, or universities. Such educational information is not included as part of the "Technical Data" that is subject to ITAR controls. Within the EAR, release of information by instruction in catalog courses and associated teaching laboratories of academic institutions is not subject to EAR.

Principal Investigators must ensure they continually monitor and update their projects in UM's [Disclosure Profile System](#) (DPS) in order to comply with conflict of interest regulations as defined by federal agencies.

³² Export Administration Regulations. [15 CFR 734.8](#) (c)

³³ 81 Fed. Reg. [35586](#), [35589](#)

³⁴ Export Administration Regulations. [15 CFR 734.8](#)

³⁵ 80 Fed. Reg. [31505](#), 31507



6.2. Study / Exchange Programs

All Foreign Person students enrolled in UM courses will undergo Restricted Party Screening (RPS) prior to participation in any study abroad or exchange programs. This applies to credit and non-credit bearing programs, activities, or trips.

UM's International Education and Exchange Programs (IEEP), or a designated responsible office, will screen students enrolling in distance education courses from outside the United States as appropriate through the UM's RPS system, for purposes of compliance with export control laws and regulations and in accordance with this Policy.

International students who never enter the United States but are enrolling in distance education courses from outside the United States will be subject to RPS. Screening will be conducted by UM's Division of Continuing & International Education, or designated responsible office.

7. INFORMATION SECURITY

Safeguarding your trade secrets, proprietary information and research is important to you, as well as UM. Therefore, it is important to protect the data that makes what you do a success as well as unique. If you are involved in cutting edge technology, developing a unique or cost-saving process, you are developing a product, or if you are collaborating with a foreign company – especially where the company is a subsidiary to that country's government... expect to be a target for espionage. The time and resources you and the Sponsor of your project have invested, as well as the data and/or product, must be protected.

Information that could be targeted may include: proprietary formulas and processes, prototypes or blueprints, research data, technical components and plans, confidential documents, computer access protocols, passwords, employee data, manufacturing plans, equipment specifications, vendor information, customer data, access control information, computer network design, software (including source code), phone directories, negotiation strategies, etc. The tactics used range from computer hacking, on-site visits, theft, photography, going through trash, elicitation, surveillance, unsolicited requests for information or participation, obtaining surplus equipment, etc.

All UM personnel are responsible for protecting information that is not public knowledge and are to be familiar with the various UM policies regarding information security found on the [UM-IT website](#), such as (but not limited to):

[POL-UMIT-EDQ-001-02](#): Electronic Data Quality Policy for Clinical Research

[A055](#): Use of Electronic Communications

[A110](#): Data Classification Policy

[A131](#): Password Security Policy

[A155](#): Information Security Policy

[A175](#): Electronic Data Protection and Encryption Policy

G-24: RSMAS Access Control Policy

7.1. Encryption

Encryption can be found embedded in hardware, such as external hard drives, as well as software technologies. UM personnel assigned to the Miller School of Medicine Campus, regardless of position, will have encryption software automatically installed on all UM-owned laptops. UM personnel who regularly use software for engineering, biometrics or other disciplines in which complex algorithms or models are created and utilized should identify if software being used contains encryption technologies. Contact the manufacturer of the software to obtain the ECCN and confirm encryption technologies. For home-grown software, employees may contact the UM's ECO for assistance.



Encryption technologies require a license for export to [embargoed/terrorist countries](#), including provision to citizens of such countries regardless of their location³⁶. Some countries restrict or ban the use of encryption technologies, which can affect whether or not UM personnel may take such items during international travel.

The following is a partial list of countries with encryption import and use restrictions. Since this information can change, UM personnel should check the U.S. Department of State website³⁷ before traveling to verify encryption restrictions or bans exist in the country that is being visited:

- Burma (license required)
- Belarus (import **and** export of cryptography is restricted. License from Ministry of Foreign Affairs or the State Centre for Information Security or the State Security Agency is required before entry.)
- China (permit required from the Beijing Office of State Encryption Administrative Bureau)
- Hungary
- Iran
- Israel (exemption for personal use, but must present the password when requested to prove the encrypted data is personal)
- Kazakhstan (A license issued by Kazakhstan's Licensing Commission of the Committee of National Security is required.)
- Moldova (A license issued by Moldova's Ministry of National Security is required.)
- Morocco (stringent controls enacted – import, export and domestic use)
- Russia (license required)
- Saudi Arabia (encryption technology is banned)
- Tunisia (import restricted)
- Ukraine (stringent controls enacted – import, export and domestic use)

UM's policy on Electronic Data Protection and Encryption is found under [Policy A175](#). UM personnel are encouraged to review this policy and other policies such as A110 "Data Classification Policy", A055 "Use of Electronic Communications", A190 "Remote Access Policy", etc.³⁸

Some items with encryption technology, such as UM-owned laptops, may qualify for an Export License Exception-TMP when travel out of the United States is for UM business³⁹. Please contact the UM's ECO for assistance in obtaining authorization.

UM personnel are encouraged to obtain a 'loaner' device from UM-IT whenever possible which does not contain encryption software. This allows the traveler to still maintain the benefits of traveling with a laptop without compromising sensitive information or violating the laws and regulations pertaining to encryption technology by the U.S. or other countries.

7.2. Collaboration Tools

In the technological age of computers, tablets, smartphones and other communication devices used for collaborating, it is important to understand the tools that are safe for sharing sensitive information.

If the online collaboration tool meets any of the following characteristics, it is okay to share sensitive information⁴⁰:

For Teleconferences:

- No recording features of any kind (audio or visual – including 'chat' or 'instant messaging')
- Attendees are restricted to invited participants; use of passcode and/or PIN required
- Document sharing is restricted to desktop display only (SharePoint is not approved)

³⁶ Obtaining an export license is not guaranteed, especially with embargoed countries. Depending on the encryption technology involved, export license may not be possible.

³⁷ USDOS (<https://travel.state.gov/content/passports/en/go.html>)

³⁸ UM-IT Policies and Procedures <http://it.miami.edu/index.html>

³⁹ Personal devices cannot be covered under License Exception-TMP, nor should any personal device such as a laptop or tablets be used to access UM files. UM personnel are liable for their own devices.

⁴⁰ UM-IT and the ECO should be consulted in advance of entering into any contract for any online subscription service, cloud storage, or other software.



Examples⁴¹ of approved tools include: Microsoft Communicator Desktop Sharing
NetMeeting Desktop Sharing
Adobe Connect Desktop Sharing
AT&T Phone Call (not recorded / assisted)

Examples of unapproved tools include: Skype, Media Hub, Hangouts, ooVoo, Paltalk, etc.

Other Collaboration Tools:

- Information is stored on secured servers located in the U.S. (no public or hybrid 'cloud'; infrastructure must be for specific users)
- Architecture is compatible with UM firewall
- Access requires permission granted by the group administrator.
- Users are required to enter a unique ID and passcode and/or PIN.
- Information transmission is encrypted

Examples⁴² of approved tools include: Blackboard (not for export-controlled items)
Box⁴³ (for EAR items only)
Daptiv (approved for ITAR items)
DEXcenter (approved for ITAR items)

UM personnel should not use e-mail accounts to share export controlled information or include screen shots of export controlled technical data. Encrypting the e-mail message may be an option, but may not be applicable in every situation. Consult UM's ECO for guidance.

7.3. Confidential Information

Release of confidential information (i.e., classified, secret, top secret) is not permitted to any person without the proper security level clearance and a documented "need to know" for that specific information.

Protecting confidential information (CI) is the responsibility of all UM personnel. CI is data that must be protected from unauthorized disclosure of public release based on state or federal law. Examples of CI data may include but are not limited to:

- Personally Identifiable Information (PII) such as name, address, phone number, email address
- Social Security Number (SSN)
- Financial Account Numbers
- Student Education Records (including schedules)
- Intellectual Property
- Medical Records
- Passwords

CI is to be used in a manner that is appropriate to your position and responsibility. Responsibilities include:

- Keep information confidential
- Keep it secure
- Distribute only with authorization
- Distribute only when necessary
- Distribute only what is necessary
- Follow encryption rules
- Assume ALL student information is confidential (because it might be!)
- Remove information that has outlived its usefulness
- Follow retention policies

⁴¹ Collaboration tools not listed that are being considered should be reviewed by UM-IT and the ECO in advance of entering into any agreement or submitting purchase requisitions.

⁴² Collaboration tools not listed that are being considered should be reviewed by UM-IT and the ECO in advance of entering into any agreement or submitting purchase requisitions.

⁴³ This is not the same as "DropBox" which is unapproved for sharing export controlled or other sensitive information by UM.



CI should not be shared with anyone within or outside the UM community unless they are specifically authorized to have it. Not all UM, personnel may be authorized to have CI, and thus verification of authorization should be obtained. Under the [Family Educational Rights and Privacy Act](#) (FERPA), educational records may be shared with other UM officials only when there is a legitimate educational interest. Some types of information may be covered under other laws such as the [Health Insurance Portability and Accountability Act](#) (HIPAA), which covers the release of medical information.

Protecting information from accidental release is what information security is all about. Following password procedures, using secured network resources, locking workstations, cabinets, and offices go a long way toward securing information.

Portable computing devices have special requirements. Since they are portable by nature, devices such as CD/DVDs, laptops, PDAs, and stick drives are routinely stolen or lost. If these devices have CI on them, theft and loss can cause significant problems unless certain procedures are followed. When using portable devices that have sensitive information;

- Ensure that the device is password protected. In the case of laptops, passwords are required to access data. In the case of PDAs or smartphones, use a PIN (the longer the better). Some PDAs allow you to enable auto-wipe of the device after so many PIN failures (10 is a good number). Files burned to CD/DVD can be password protected (see Encryption section below).
- Ensure that the CI on the device is encrypted. Most smartphones do NOT offer encryption at the file level and should not be used to store CI. If you need to store large quantities of CI, your department will need to invest in a portable storage device with encryption technologies.⁴⁴
- If you do lose CI on a portable device, you must report the loss or theft immediately to your supervisor, UM-IT and all interested parties⁴⁵.

Every time CI is distributed, there is a risk of disclosure. Most CI releases occur accidentally, that is, the sender did not realize they were sending CI. Unfortunately, electronic distribution (e.g., e-mail) cannot be undone. If you must distribute CI, follow these guidelines.

- Distribute only when necessary.
- Consider non-electronic or “on demand” delivery. Is it possible and reasonable to send the information via paper? Can receivers “query” the information only when they need it?
- Limit the distribution ONLY to information that is needed. If someone needs a list of email addresses, do you REALLY have to send them address, phone number, and grade information? If someone needs a list of all students in the sailing club that have a below 2.5GPA, do you have to send them the *actual* GPAs or is the list of the students’ names that don’t meet the criterion sufficient?
- Encrypt and password-protect the information before sending.

7.4. Classified Research

PIs should understand that Classified Research typically will not allow negotiation of the award terms and will likely impose strict requirements such as no foreign person participation, publication restrictions, workspace security, ISO-9000 compliance, etc. PIs should consult with their Department Chair, Dean, and the ECO in advance of submitting proposals and accepting awards for such endeavors. The ORA, in consultation with the President and General Counsel, will have final authority in approving all research identified as “classified”.

All proposals for classified research will be processed through the Office of Research Administration and Fiscal Management, as with all research proposals. If there is question as to whether the research does or does not contain classified information, the PI must obtain written clarification from the Sponsor prior to submitting the proposal. Whenever a U.S. Department of Defense DD Form 254, *Contract Security Classification Specification*, is requested to be completed by Office of Research Administration (ORA), Fiscal Management or a researcher, the ECO and the Facility Security Officer⁴⁶ shall be notified and provided a copy of the completed DD-254.

⁴⁴ Portable storage devices with encryption technologies will be restricted to some foreign persons and may require a license to travel with to certain international destinations.

⁴⁵ “interested parties” may include HIPPA office, General Counsel, Vice Provost for Research, etc.

⁴⁶ Facility Security Officer is Raul F. Garcia-Casariago.



The PI should allow adequate timing for review to be completed by all parties involved of approximately 3-4 weeks, or more.

For any research or other agreement involving Classified or other Government restrictions, the ORA, ECO, and General Counsel shall be included among the limited UM personnel who require the proper security clearance to have access to and discuss all elements of the work being performed by UM.

7.5. Unclassified Information

The term sensitive unclassified information is an informal designation applicable to all those types and forms of information that, by law or regulation, require some form of protection but are outside the formal system for classifying national security information.⁴⁷ As a general rule, all such information may be exempt from release to the public under the [Freedom of Information Act](#) (FOIA).

The U.S. Department of Defense also uses the term Controlled Unclassified Information (CUI) to refer to certain types of sensitive information within the DoD that require controls and protective measures. CUI includes “For Official Use Only” (FOUO) and information with comparable designations that is received from other agencies, DoD Unclassified Controlled Nuclear Information, “Sensitive Information”,⁴⁸ and DoD technical data.⁴⁹

“Controlled Unclassified Information” (CUI) is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interest of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces “Sensitive But Unclassified” (SBU).

7.6. Cloud Computing / Online Data Storage

“Cloud computing” and other types of digital data storage on remote servers are services that are being promoted as ways to reduce costs as well as to leverage computational capabilities and to facilitate digital data sharing. Generally speaking, cloud computing refers to the use and access of multiple server-based computational resources via a digital network such as the internet. Remote storage refers to services limited to storage and backup of digital data on a third-party server. A third-party server is something that is owned and maintained by someone other than UM.

On June 3, 2016, the Department of Commerce’s Bureau of Industry and Security (BIS)⁵⁰ and the Department of State’s Directorate of Defense Trade Controls (DDTC)⁵¹ issued new rules revising existing definitions and adding new ones in the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). The new rules, part of the Administration’s Export Control Reform Initiative, seek to enhance clarity, promote consistency of terms across the two export control regimes, and update the EAR’s treatment of electronically transmitted and stored technology and software.

The BIS Final Rule went into effect – September 01, 2016, and references to “exports to the cloud” are located in EAR Part 734.18 “Activities that are not Exports, Re-exports, or Transfers”, provided that transmitting or storing electronic data that meet certain security standards would not constitute an export of that data, provided that the technology or software is:

1) Unclassified; (2) Secured using "end-to-end encryption"; (3) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its

⁴⁷ The U.S. Department of State uses SBU as a document designation comparable to For Official Use Only (FOUO).

⁴⁸ Defined in the Computer Security Act of 1987 ([Public Law 100-235](#))

⁴⁹ DoD [Regulation 5200.1-R](#), Information Security Program

⁵⁰ [81 Fed. Reg. 35586](#)

⁵¹ [81 Fed. Reg. 35611](#)



successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other equally or more effective cryptographic means; and (4) Not intentionally stored in a military-embargoed country or in the Russian Federation.

Thus, transmission of **controlled technology and data to, or storage in, a foreign country under these conditions no longer constitutes an export. As ongoing (i.e., end-to-end) encryption is a requirement for this safe harbor provision, the EAR now include a definition of “end-to-end encryption” as (i) the provision of cryptographic protection of data such that the data are not in unencrypted form between an originator (or the originator’s in-country security boundary) and an intended recipient (or the recipient’s in-country security boundary), and (ii) the means of decryption are not provided to any third party.** The originator and the recipient may be the same person. Transmissions within a cloud service infrastructure also fit within this safe harbor provision when the transmission is made from one node or cloud infrastructure element to another, provided that it was appropriately encrypted before any data crossed a national border.

The rule also includes a definition for “access information,” which is information (like decryption keys, network access codes and passwords) that would allow access to encrypted technology and software in unencrypted form. Such access information is subject to the same level of export controls as the data being accessed if the data were un-encrypted. The rule also clarifies that a victim of a data or security breach related to encrypted data is not considered responsible for the export, reexport, or transfer of that data, provided that the originator of the technology did not provide access information or otherwise permit access to the encrypted data.

Such revisions make feasible a wider variety of cloud computing and cloud storage solutions, and significantly simplify associated compliance with export controls, relative to EAR controlled technology and software. However, the EAR also contain an important limitation that releasing decryption keys or other access information that will permit a foreign person access to technology or technical data will constitute an export and be subject to the export control restrictions applicable to the foreign country in question. It is important to keep in mind that these changes do not apply to ITAR controlled technical data, with respect to which restrictions on the use of the cloud have not changed. It remains critically important that UM personnel work with the ECO to determine and to distinguish between EAR controlled technology and software, on the one hand, and ITAR controlled technical data, on the other hand, when considering the use of cloud services.

Before engaging service agreements with any cloud service / online data storage provider, UM-IT should be consulted first to confirm that there are no internal resources available to meet the access and storage needs of the department/employee. Only if UM-IT is unable to provide the resources needed will entering into an agreement with a cloud service provider (CSP) be considered. Obtaining disclosure from the provider of where the servers and routers are located will be required, the type of infrastructure, and review of how the service will be used will need to be reviewed by UM-IT and the ECO in advance of entering into any contractual arrangement and submitting the initial purchase requisition. .

7.7. Laboratory Information Security

No photographs of export-controlled, restricted, confidential, proprietary, or unclassified items are allowed. All cell phones must remain off and stored while in an access-restricted room.

No passwords are to be taped to computer monitors, keyboards, or other areas near computers. Personnel are to memorize the password needed to gain access to certain folders, shared drives, or other secured sources. Passwords must conform to UM policy⁵².

Removable hard drives may be used for data backup. When not in use, removable backup drives will be securely locked in a container in an access restricted location.

Removable hard drives should contain encryption technologies within the hardware to ensure added security.

⁵² UM-IT Policy A131 “Password Security Policy” <http://it.miami.edu/index.html>



When not in use by authorized researchers, laboratory notebooks and any hard copies that contain controlled, restricted, proprietary, confidential technical data will be securely locked away in a location with restricted access.

All UM personnel are to take security precautions with computers (desktop, laptop or tablet) **before** any export-controlled technical data or export-controlled software is downloaded. If the computer is connected to the UM network, all electronic devices being used – including smartphones, tablets, etc.- are to have UM-IT approved encryption software installed and activated at all times.

8. CONTRACTS AND AWARDS

Most data and information involved in UM research can be excluded from export control regulations under the EAR or ITAR **if** they qualify under the following provisions (Ref. [section 6.1](#) of EMCP):

- (a) the Public Domain Exclusion
- (b) the Fundamental Research Exclusion (FRE)
- (c) the Exclusion for Educational Information (EEI)

It is important for researchers and others involved in research to be aware of these key exclusions and to understand that their benefits can be lost if certain provisions are present in research-related agreements. For this reason, PIs should avoid entering into informal understandings or “side agreements” with research sponsors that restrict foreign person access to the research or that impose sponsor controls on the publication or other dissemination of research results. It is also important to note that the restrictions enforced by OFAC are not affected by the ITAR, EAR, or the FRE.

It is highly recommended that UM personnel review the proposal, notice of award, and any other binding agreement carefully for references to export controls, security, fundamental research and/or restricted research. If the proposed research meets the definition of fundamental research, which is excluded from the licensing requirements of export controls, this applicability to the FRE should be noted on the proposal document.

Engaging in non-fundamental research creates intersection with export control laws and places the student’s graduate work (thesis/dissertation) at risk, as well as their ability to graduate. Export controlled, non-fundamental research projects require the establishment of a Technology Control Plan, export compliance training for all research staff, and implementation of security protocols to protect the research from inadvertent releases. Please review [Appendix C](#) “Export Compliance Decision Tree for Administration of Contract Provisions of Concern” for additional guidance.

8.1. Proposal Contract Routing Forms

UM’s Office of Research Administration (ORA) manages the [Proposal Contract Routing Form \(PCRF\)](#)⁵³, which includes a section called “Export Control Information” containing five (5) questions to be answered by the applicant. UM’s ECO uses the answers to these questions, along with other information, to review for applicability to export controls. This process will help to determine whether licensure and/or other security measures are required should the project be awarded. ORA will be responsible for notifying the ECO when the project has been awarded in order to review contract language and address any export control issues that may exist. Export control issues must be addressed prior to executing any research agreement or contract.

ORA will send to the ECO for review any PCRF, along with supporting documentation (e.g., scope of work, budgetary documents, sponsor terms, etc.), that meets any one of the following criteria before submitting the proposal:

1. Is the Sponsor a branch of the military or other high-ranking federal agency? (For example: ONR, NASA, DOD, Army, NOAA, , DARPA, DOE)
2. Does the research fall outside of basic or applied science? (For example: developing or testing a product for commercial market or military applications)
3. Is any of the equipment to be used and/or purchased high-end technology? (For example: high-energy lasers, acoustic devices, navigational devices, Satellite images / equipment, etc.)

⁵³ The PCRF Form is mandatory for all research projects and is completed electronically on-line for all new requests and updates.



4. If traveling internationally, will it be to any embargoed or restricted country? View list at: http://www.pmdtc.state.gov/embargoed_countries/index.html
5. Will the research be for marine science where research conducted takes place in International Waters? (12nms from U.S. shores is the point at which items have been exported out of the U.S.)
6. Will the research require the use of Select Agents and/or Toxins identified by the Government's DURC Policy? (Refer to [section 5](#) above)

Approval by the ECO is required before the proposal can be submitted. Reviews by the ECO will be completed **within 5 business days of receipt**, provided there are no extenuating circumstances or additional information is not pending. PIs may send the PCRF and supporting documentation directly to the ECO in advance.

NOTE: For proposals with export control concerns, PI's should anticipate **5 business days** for review by the ECO. Proposals under export control review may not be submitted until cleared by the ECO.

If the PI is unsure how to respond to the export compliance questions, the following guidance is provided. When there is doubt how to answer the questions, the PI should contact the ECO directly for assistance. Answering falsely to any of the questions could put the PI, the project, and/or the project staff at risk for violations against the Arms Export Control Act.

Question #1: ***Will this project require any of the project staff to travel to a country that is identified as restricted or embargoed by the U.S. Government?*** The PI will click on the included hyperlink and review the list of countries on the website. If the country(ies) in which research activities will take place is listed, check "YES" on the PCRF.

Question #2: ***Will this project involve research activities in International Waters?*** A hyperlink to the U.S. Maritime zones and boundaries is included as reference. However, if research conducted from a research vessel or other watercraft extends beyond 12 nautical miles from the U.S., check "YES" on the PCRF.

Question #3: ***Will the research require the use of select agents and/or toxins identified by the U.S. Government's DURC Policy?*** UM Personnel who are not familiar with this policy should access the embedded hyperlink and review the details of the DURC. The PI may also review the [section 5](#) above on DURC for additional guidance.

Question #4: ***Will the project include high-energy lasers, acoustic and/or navigational devices, satellite images and/or equipment, non-public source code, nanotechnology, or any other high-end technology/technical data?*** This question is bound to give many PI's some difficulty, unless they already have a database or spreadsheet of the items they currently have on hand or have obtained the ECCN in the quote of the items they have identified that will need to be procured. The PI may access the hyperlink that is included in the question for a general search, but should consult with the ECO to answer this question appropriately.

Question #5: ***Will there be any person involved in the project that is not a U.S. Citizen or Permanent Resident and is a national of Cuba, China, Syria, Sudan, Iran or North Korea?*** Both conditions must be met to answer "YES" to this question. This applies to all persons working on the project, including UM personnel, UM students, and any person/entity that will be subcontracted in the project. Entities who are not a U.S. registered business would also qualify as a foreign person.

8.2. Restrictive Clauses

Certain research agreement provisions may negate the FRE and require seeking a license or undertaking monitoring and other activities. These clauses are identified on the UM Export Control Decision Tree ([Appendix D](#)) and are summarized below. If any of the following provisions are present and negotiations to change are unsuccessful in a research agreement or subcontract, a material transfer agreement (MTA) or non-disclosure agreement (NDA) related to research, the document will be required to be reviewed by the ECO and the General Counsel's (GC) office, as well as any other appropriate UM office.



- (a) Sponsor maintains the right to restrict or approve publication or release of research results. (This does not include the brief delay to protect a sponsor's confidential information or to preserve the patentability of an invention).
- (b) Research data and/or other research results will be owned by the sponsor (e.g., a sponsor's proprietary or trade secret information).
- (c) Statements that export control regulations will apply to the research.
- (d) Incorporation by reference of Federal Acquisition Regulations (FARs), agency-specific FARs, or other federal agency regulations, which impose specific controls on access to dissemination of research results.
[\(See Appendix D\)](#)

NOTE: Awards that contain export control concerns, PI's should anticipate **5 business days** for review by the ECO. Awards under export control review may not be executed until cleared by the ECO. Funding may be withheld until compliance measures⁵⁴ are fully implemented.

8.3. NASA & China Affiliation

The National Aeronautics and Space Administration (NASA) is restricted by specific applications of Section 1340(a) of The U.S. Department of Defense and Full-Year Appropriations Act, Public Law 112-10 and 112-55, and Section 539 of the Consolidated and Furthering Continuing Appropriation Act of 2012, from using funding appropriated in the Acts to enter into or fund a contract of any kind to participate, collaborate, or coordinate bilaterally in any way with China or any Chinese-owned company, at the prime recipient level or at any sub-recipient level, whether the bilateral involvement is funded or performed under a no-exchange of funds arrangement. Awards which used funding that was appropriated after April 25, 2011, either as a new award or through a modification, are subject to this restriction.

The restriction, for UM purposes, applies to any collaborations, funded or unfunded, with China (People's Republic of China), any Chinese government run enterprises, any company or university incorporated under the laws of China, or individuals in any way affiliated with these entities. The restriction does not apply to the purchase of commercial or non-developmental items.

Any activities that involve Chinese collaborators or visitors that could fall within the "collaborative" area (funded or unfunded) that are part of any projects that receive NASA funds or use the results of NASA funded projects will need to be reviewed by ORA and Export Control & Technology Management. Approval will also be required from NASA in writing.

One can independently analyze this restriction and ponder, "what entity is paying for the Chinese visitor/collaborator/participant work or visit while at UM?" For example, if a Chinese visitor is on sabbatical or is a post doc from a Chinese university and the Chinese university is paying their salary, the visitor will be restricted from working on a NASA funded project. However, if they are being paid by a U.S. institution or they are not affiliated with China or a Chinese owned company, they would be eligible to work on NASA projects. A permanent resident would not be restricted from working on a NASA funded project as long as they are working for a university or company established under U.S. law.

All PIs will be required to disclose their compliance with the NASA China Funding Restriction. Disclosure is to be made on all proposals as well as prior to NASA's issuance of any new or renewal NASA awards. This is to ensure the information disclosed remains accurate throughout the term of the project. The PI is to certify that s/he will not participate, collaborate, or coordinate bilaterally with the Chinese government, any Chinese-owned company, any Chinese university, or individuals affiliated with these, at the prime recipient level or any sub-recipient level, whether the bilateral involvement is funded or performed under a no-exchange of funds. Exceptions will require approval by ORA, UM's ECO, and NASA.

The NASA China Funding Restriction disclosure must be obtained when UM is the primary applicant and must certify compliance on behalf of the entire team, including all sub-recipients. The PI with the assistance of ORA should review each unfunded collaborator that s/he may want to work with to determine if that collaborator is

⁵⁴ Compliance measures may include instituting a TCP, securing an export license, conducting RPS, installing proper security measures, etc.



restricted from working on the NASA project per NASA's appropriation guidance. When in doubt, the project manager at NASA should be consulted and the ruling is to be obtained in writing.

The following are provided as guidance from the law itself as well as interpretations from NASA.

1. No person on a J-1 visa from China may work on any NASA award, including collaboration agreements and agreements where no funds are exchanged.
2. No person (regardless of nationality) with an affiliation with a Chinese institution, including adjunct faculty, may work on a NASA award. Determinations of whether or not status of "honorary faculty" with a Chinese institution is an "affiliation" shall be determined on a case by case basis by NASA directly.
3. Those persons on a J-1 visa from China, and those with a Chinese affiliation, may not use equipment, software, etc., purchased using NASA funds on a restricted project.
4. Although commercial items of supply may be procured in and from China as needed, no subcontracts are allowed for research or consulting on NASA projects.
5. NASA funds cannot be used for travel costs or otherwise to support direct collaboration between an investigator and any person employed by a Chinese institution; no matter what their citizenship. The cost of attending multi-national conferences held in China may be acceptable, but require pre-approval from NASA in writing. Approval must accompany eBERFs submitted in order to be reimbursed⁵⁵.

8.4. Debarment / Restricted Persons

[Executive Order 12549](#) called for the creation of a government wide debarment and suspension system in connection with all transactions with federal agencies.⁵⁶ Debarment and suspension are actions taken by the federal government against organizations or individuals who have committed fraud or a criminal offense in violation of federal law. The regulations require that the UM (considered the formal applicant for grant and contract funds from the federal government) certify that neither UM, its officers, nor researchers⁵⁷:

- a) Are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions (defined as being eligible to receive federal funds) by any federal department or agency.
- b) Have, within a 3-year period preceding an application for funding, been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain or performing a public transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property.
- c) Are presently indicted or otherwise criminally or civilly charged by a government entity (federal, state or local) with commission of any of the offenses enumerated in (B) above.
- d) Have, within a 3-year period preceding an application, had one or more public transactions (federal, state or local) terminated for cause or default.

Any individual who meets any of the conditions outlined above (a-d) must **immediately** notify their direct supervisor, the Department Chair/VCA/Dean, the Office of Research Administration, the Office of the Vice Provost for Research, and the General Counsel's Office⁵⁸. In addition, the individual is precluded from receiving federally funded grants or contract awards as well as being paid with federal funds.

⁵⁵ UM policy [BSL-070 "International Travel Approval & Authorization"](#) or <https://miamiedu.sharepoint.com/sites/bf/Pages/Treasury-Policies.aspx>

⁵⁶ Other related regulations are: [15 CFR Part 736](#) – General Prohibition Four, [15 CFR Part 744](#) – Control Policy: End-User and End-Use Based, [15 CFR Part 758.3](#) – Responsibilities of parties to the transaction, [45 CFR Part 76](#) – Government Debarment and Suspension (Non-Procurement), [48 CFR Parts 9 & 52](#) – Federal Acquisition Regulation; Uniform Suspension and Debarment Requirement.

⁵⁷ The "applicant" is UM. The "officers" or principals are trustees and senior administrative staff. The "researchers" are the faculty and their professional colleagues who undertake such research activities.

⁵⁸ Reference Employee Handbook



All research personnel (UM and non-UM) are to be screened against federal debarment and suspension lists through UM's RPS system before any federal funds are released. Screening processes will be completed by the ECO or other designated office.

9. RESTRICTED PARTY SCREENING

Federal Regulations require that businesses screen and verify the parties for which they are doing business with do not appear on any denied/restricted/debarred list.⁵⁹ The U.S. Government maintains various lists of entities for which there are restrictions on doing business. The Bureau of Industry and Security (BIS) recommends that these lists be reviewed to ensure that a proposed transaction does not violate regulations. UM personnel are responsible for ensuring that foreign persons or entities (including students, visitors, observers, outside services vendors, etc.), have been screened, prior to engaging in business activities, to confirm that the person or entity does not appear on any agency list of denied/excluded parties.

[Amber Road](#) is the official provider of restricted party screening compliance for UM.⁶⁰ The administrator for this tool is UM's [Export Compliance Director](#). UM departments that need to conduct screenings on a regular basis may submit a request for access. Otherwise, requests to conduct a screening on a person or entity may be submitted to the exportcontrol@med.miami.edu. Requests to conduct RPS are to be submitted on form [EXPORT-F-006](#). Requests will be completed within 2 business days.

Persons / Entities determined on a denied/excluded party list will first be investigated to ensure that the result is a true match⁶¹. Even a true match may not mean that no UM business can be conducted with such persons. Specific license requirements, terms and conditions, or other factors may apply. UM will conduct detailed due diligence to ensure full compliance with the restrictions for the parties on these lists.

The RPS system performs screening against all relevant U.S. Government lists, including: Department of Treasury Office of Foreign Assets Control (OFAC), Department of State, Department of Commerce, Department of Justice, Food and Drug Administration (FDA), Immigration and Customs Enforcement (ICE), Federal Bureau of Investigation (FBI), Office of Inspector General (OIG), Department of Health and Human Services (HHS), General Services Administration (GSA). The software also screens against lists from foreign governments. There are over 200 lists that the system screens against simultaneously. Lists are continuously maintained by Amber Road.

The RPS system currently does not include State lists such as the Florida Agency for Health Care Administration ([AHCA](#)) or the Florida Department of Law Enforcement ([FDLE](#)). Screening of State lists will need to be conducted directly by the UM department requiring such screening to be completed. Background criminal investigations will need to be requested through UM's [Security](#) department.

9.1. Authorized Users

The ECD is the RPS system administrator. Access to the RPS system will be given by the administrator when evaluation of the need has been determined and approved by the ECD. All users will be given "Ad-Hoc" privileges which will allow for one-time screening capability. Departments who maintain lists for continuous screening will identify 2 users within the department who will be given administrative privileges in order to maintain comma-separated values (CSV) formatted lists accordingly for their department.

On an annual basis, a list of users will be sent to the department/unit head or designee to confirm that the individual(s) listed are still appropriate authorized users for the specific department/unit. However, the department/unit should notify the ECO as changes in authorized users occurs.

⁵⁹ [Executive Order 12549, 15 CFR Part 736](#) – General Prohibition Four, [15 CFR Part 744](#) – Control Policy: End-User and End-Use Based, [15 CFR Part 758.3](#) – Responsibilities of parties to the transaction, [45 CFR Part 76](#) – Government Debarment and Suspension (Non-Procurement), [48 CFR Parts 9 & 52](#) – Federal Acquisition Regulation; Uniform Suspension and Debarment Requirement.

⁶⁰ No UM office or personnel should be using Visual Compliance (eCustoms) or other RPS subscription service.

⁶¹ Due to commonalities within the search criteria, the search result may need to be further investigated to confirm if the result is indeed for the individual/entity being screened.



9.2. “Hits”

Authorized users are to conduct screening in accordance with their department’s internal procedures, which should also be aligned with UM’s Export Compliance policy and procedures. If there is a possible match of the party being screened with an entry on any of the lists in the RPS system (a “hit”), a secondary person within the department should verify that it is a possible match by screening with additional detailed information to confirm.

If the ‘hit’ cannot be ruled out on secondary screening, other available information should be used such as date of birth, professional license number, address, and/or photo (if available). If the hit still cannot be ruled out, the possible match should be forwarded to the ECO for final review, along with the criteria used to determine the possible match.

The departments of authorized users are responsible for maintaining records of determinations that are not forwarded to the ECO. The records are to be maintained per [section 16](#) of this document.

9.3. USCIS I-129 Attestation

Effective February 20, 2011, the U.S. Citizenship and Immigration Services (USCIS) issued new requirements for employers sponsoring foreign persons through the I-129 Petition for a Nonimmigrant Worker process. Specifically, the revised I-129 form added Part 6, “Certification Regarding the Release of Controlled Technology or Technical Data to Foreign Persons in the United States.”⁶²

This new required attestation stems from the Deemed Export Rule under the EAR and the ITAR, which provides that the transfer, release, or disclosure of controlled technical data, technology or software to a citizen or national of a foreign country, even if in the United States, is ‘deemed’ to be an export to that country. However, inclusion of the Part 6 of the I-129 application is the first time export control determinations have been an explicit part of the immigration process as directed by USCIS.

The I-129 Export Control Attestation form ([EXPORT-F-001](#)) is included with UM’s visa-application process for foreign persons, which includes screening through the RPS system. This form is to be completed by the applicant’s supervisor since they are most knowledgeable of the day-to-day activities and risks to controlled items. It is the responsibility of the supervisor to monitor changes in job descriptions and/or departmental procedures that may put a foreign person at risk of exposure to controlled or restricted items. If the applicant will be at risk for exposure to controlled items, the supervisor will be required to minimally, attend *Export Compliance Basics* training. (See [section 14](#) of this document)

Along with the completed I-129 attestation form from the supervisor, the applicant’s job description and CV/Resume will be submitted for review. **The applicant will not be able to move forward with the Visa application process until the I-129 attestation review has been completed.** Thus, it is important to complete and submit the required documentation as quickly as possible so the visa application process is not delayed.

If the supervisor is unsure how to assess the export control risks that may exist within the department, s/he should contact the Export Control & Technology Management office for assistance. **Not knowing does not mean a “no” answer on the attestation form.** Reviewing contracts and agreements is the first place to start in assessing export control risks. Technology Control Plans (TCP) should be in place to help mitigate risks of releasing (or exporting) the controlled items.

For additional guidance, the I-129 Export Control Attestation SOP ([EXPORT-S-001](#)) is available to review on UM’s Export Control & Compliance website [“Policies & Forms”](#) page along with the form ([EXPORT-F-001](#)).

⁶² [USCIS FAQ about Part 6 of Form I-129](#)



9.4. Vendors

Vendors in the UM Purchasing vendor database must complete a UM Vendor application form.⁶³ All firms selling materials, equipment and/or services will be required to submit a vendor application and be approved by UM's Purchasing department before engaging in UM business. As part of the approval process, all vendors will be screened through the RPS system by authorized users within the Purchasing department. If a match is found against any of the lists which the system screens against, Purchasing and the ECO will review the vendor to confirm it is an exact match and decide if the vendor will be allowed the opportunity to conduct business with UM.

Vendors are expected to conduct themselves in accordance with fair, ethical and legal trade practices when doing business with UM. This includes compliance with U.S. export control laws and regulations. When requested by UM, Vendors will be required to supply export control classification numbers (ECCN) for all products they supply to UM as per [15 CFR 758.3](#), and submit the information on form [EXPORT-F-002](#), "Export Classification Certification." Failure to provide the information could result in freezing the vendor's UM account and institute denial of current and future business transactions.

10. PHYSICAL SECURITY & PERSONNEL ACCESS

UM is dedicated to providing a safe and secure environment for all who study, conduct research, live and work at any of its campuses. The safety and security of UM's physical space and assets is a shared responsibility of all members of the UM community. UM personnel should be familiar with the [Access Control Policy for each campus and office](#).

10.1. Campus Access

The UM appropriate campus access control authority is responsible for processing all facility access requests.

Foreign person personnel / visitors are not permitted in export controlled areas without:

- a. Prior export authorization; and
- b. An escort by UM personnel who is a U.S. citizen or Permanent Resident as applicable; and
- c. Necessary badging or identification as required in accordance with UM campus access control authority processes⁶⁴ and/or departmental policy.

PI or functional delegate is responsible for ensuring that all foreign persons permitted to work in an export controlled area have been approved under separate U.S. and/or local export authorization prior to access of any export controlled equipment or data; and

PI or functional delegate must ensure that all foreign persons are escorted and managed as applicable when working in any environment where export controlled equipment and/or data reside (e.g., labs, work areas).

- o UM personnel who are a U.S. citizen or U.S. Permanent Resident must escort all foreign person employees / visitors if they are required to go beyond their designated areas of their access, or require access beyond the authorized hours in the facility.
- o A critical phase of a site security program is the extent to which visitors are granted access to information, and permission to enter sensitive or compartmentalized areas within the site. In most cases, this is determined by the host of the visitor, and should be based strictly on clearance status and "need to know" of the visitor.
- o Visitor access is limited to only those who have been identified, hosted and escorted by authorized UM personnel. The authorized escort is required to maintain constant observation and supervision over visitors during tours, meetings, or other visitation needs. The escort is responsible for any visitor he/she escorts on UM property.

⁶³ UM Purchasing Department "Vendor's Corner" website. http://www.miami.edu/finance/index.php/purchasing/vendors_corner/vendor_forms/

⁶⁴ UM Medical Campus Security [policy A-045](#) "Campus ID/Badge & Access Cards", [UM Policies B040 & B045](#) "Identification Cards: Employees & Retirees", RSMAS policy G-24 "Access Control Policy"



When required, compartmentalized areas should be established by the responsible department in order to control access and enhance physical security. Installing access-control card readers in these areas will also provide a medium to restrict unauthorized access. Card reader access should be given only as part of the permanent badging process.

10.2. Foreign Persons

For activities where an export control license is required under either the EAR or ITAR, no foreign person will be given access to material that involves the disclosure of technical data as defined in the regulations until authorization from the U.S. Government has been obtained.

UM personnel who have supervisory responsibility for foreign persons will be knowledgeable on the activities affecting foreign persons which are pertinent to their activities. In addition, supervisory personnel will brief other employees under their direction concerning restrictions relating to foreign persons so that no technologies and/or technical data are transferred without proper authorization.

Foreign persons will be informed by their supervisor when an export license is required from the U.S. Government before they are given access to hardware, software, or other technology or technical data. In addition, foreign persons will be informed of their responsibility to treat the technology and technical information obtained during their employment or visit in accordance with UM procedures for the protection of sensitive items.

An individual who is a citizen of more than one foreign country, or has citizenship in one country and permanent residence in another, as a general policy, the last permanent resident status or citizenship obtained governs. Where status of a foreign person is uncertain, UM's ECO will contact the U.S. Government to determine where the stronger ties lie based on the facts of the specific case. This may require investigation into the foreign person's family, professional, financial and employment ties.

10.3. Identification Badges

All UM personnel are required to possess a UM ID card/badge while on any campus. While anywhere on the Medical Campus, all UM personnel are required to have a UM-issued ID card / badge displayed on the front of their person in an immediately visible manner.⁶⁵

Any person who is within an access-controlled area without possessing (or on the Medical Campus properly displaying)⁶⁶ a UM-issued ID Card/Badge must immediately be reported to the respective campus security authority who will take appropriate action which may include authorization verification or removal from the area.

All badges are issued by Security to authorized personnel. Access to UM facilities is subject to revocation at any time without prior notice.

10.4. Campus Tours / Visits⁶⁷

UM encourages visits to any of the campuses; however, there are certain areas that are restricted to the general public and/or unauthorized persons who can include UM personnel and students. When extending an invitation to visit or tour any UM campus due diligence must be accomplished to ensure that the safety and protection of UM research, assets, and personnel are maintained. Please review the decision tree at [Appendix I](#) for assistance with export controls and international visitors.

BEFORE the visit, the Host must:

- Have all visitors screened through RPS. (Submit request [EXPORT-F-006](#))
- Identify all areas that the visitors will be present.
- Areas that are not under the Host's authority, the host must obtain approval from the department administrator – ensuring that no area is restricted.

⁶⁵ [UM Security policy A-045](#) "Campus ID/Badge & Access Cards", UM Policies B040 & B045 "Identification Cards: Employees & Retirees"

⁶⁶ [UM Security policy A-045](#) "Campus ID/Badge & Access Cards", UM Policies B040 & B045 "Identification Cards: Employees & Retirees"

⁶⁷ Public tours and student orientation tours view common areas only and thus do not apply to this section.

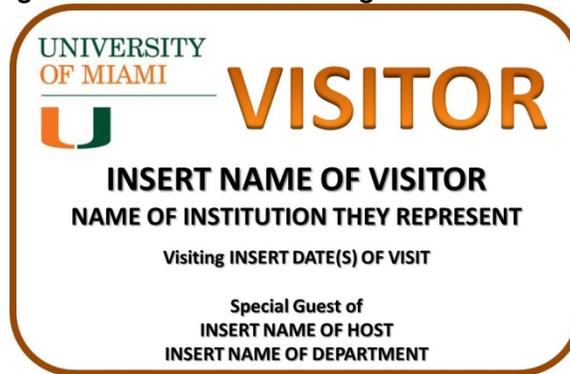


- Before visiting any lab area, the Host is to ensure that no export controlled, restricted, confidential and proprietary or other sensitive items will be present or exposed to the visitors.
- Verify with UM Security any special protocols that may be needed.

DURING the visit, the Host must:

- Keep visitors to approved areas.
- Remind visitors there is no photography allowed in lab areas.
 - Provide plastic sealable bags for visitors to put cell phones in to ensure cameras or other recording applications on these devices are not enabled during tour.
- (Optional) Provide each visitor with an ID badge (similar to that which is provided at conventions)

Sample ID Badge that can be created using Microsoft Word:



Unsolicited requests to visit UM campuses and labs should be carefully scrutinized. Review and approval is to be obtained from the Department Chair and Export Compliance Director prior to accepting the unsolicited request. Such requests are often part of espionage activity.

11. TECHNOLOGY & TECHNICAL DATA

Technology is defined as, “specific information necessary for the “development”, “production”, **or** “use” of a product. The information takes the form of “technical data” or “technical assistance”⁶⁸. In essence, it is any information that someone would need to make or use controlled goods.

Technical Data may take the forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions spoken, written or recorded on other media or devices such as disk, tape, read-only memories (ROM).

Export of technology is controlled according to the provisions of each Category⁶⁹. However, technology required for the development, production or use of a controlled product remains controlled even when applicable to a product that is controlled at a less restrictive level.⁷⁰

11.1. Purchase Requisitions

It is imperative to understand when export-controlled items (software, equipment, technology) are present. To help identify items that are of risk, export control review is conducted on UM purchase requisitions where items are of concern. Not all items require review ([See Appendix E](#)). UM’s Purchasing Department is responsible for identifying items requiring review, or consulting with UM’s ECO prior to issuing a Purchase Order (PO) for the submitted requisition⁷¹.

⁶⁸ Technical assistance may take forms such as instruction, skills, training, working knowledge, consulting services. It may also involve transfer of “technical data”

⁶⁹ Controlled technology is that which is listed on the [Commerce Control List](#) (CCL)

⁷⁰ Export Administration Regulations [15 CFR 772](#)

⁷¹ Reference [EXPORT-S-002](#) “Export Compliance Review Process for Purchase Requisitions”



11.2. Inventory & Tracking

Each department is directly responsible for the control, use and security of movable equipment in its possession. In accordance with this responsibility, each department is to designate a property administrator to facilitate processes and communication. The department's property administrator or designee and others who are directly involved in equipment purchasing and inventories should be familiar with UM policies and procedures. Per [Policy B053](#), "Annual Equipment Verification Instructions and Approval Submission", departments are to do an annual inventory between the months of September and December to verify equipment and inventory by utilizing the equipment system in [Property Accounting](#). Departmental property administrators can download their equipment inventory from the Moveable Equipment System in UM-APPS⁷².

Once the inventory is downloaded from UM-APPS, the property administrator can use the "create spreadsheet" option and export to an Excel sheet. Within the spreadsheet, a new column can be added for ECCN and HTS Code to further enhance the department's equipment inventory information.

For items that fall outside the moveable equipment database, departments may also utilize the Inventory & Tracking form located in [Appendix F](#) of this policy to manage all assets and other items they have in their possession. This form may also be adopted into a Microsoft Access database that can provide easier electronic inventory management from cradle-to-grave.

EHS maintains a biological and chemical inventory database that identifies the name of products and materials, quantity of products and materials, purchaser, location where such products and materials are stored and used on campus.

All chemical, biological and radiological purchase requisitions must be reviewed and approved by the appropriate overseeing department (e.g., Radiation Control Center) prior to purchase and delivery onto campus.

11.3. Shipping

It is the responsibility of all UM personnel who are shipping items outside the United States (including hand-carrying items) to comply with export control laws and regulations. Any transfer of export-controlled items by any method may be subject to export control restrictions and may require an export license or may be prohibited depending on the item, destination, recipient, and/or end-use. Even if an item is cleared through the U.S. Customs and Border Patrol (CBP), an export license may still be required.

Shipping to countries subject to embargoes must first be cleared by the Export Control & Compliance office. UM personnel who are responsible for shipping packages out of the country should obtain a list of contents before shipping and contact the ECO with any questions. One should not ship an item without taking the time to do due diligence and ask the ECO to determine if a license is required.

Mislabeling the package or misrepresenting the classification of the item(s) being shipped is illegal. Reporting an incorrect export value on a Shipper's Export Declaration (SED) and/or Commercial Invoice is a violation of export regulations. A shipping decision tree can be found in [Appendix G](#) of this Policy for shipping-related questions and concerns. Any potential export control issues regarding shipping should be referred to the ECO.

In addition to the export control classification numbers for items being exported, the [Harmonized Tariff Schedule](#) (HTS) codes for each and every item being exported needs to be applied and entered on shipping documentation. While each country has its own HTS, the USHTS codes may also be used when items are being imported into the United States. Shippers may use a search-friendly web-based tool for determining HTS codes, www.HTSCode.org. However, the U.S. International Trade Commission's listing of HTS codes⁷³ should also be consulted for confirmation of what is provided by www.htscode.org.

HTS Codes provide a detailed description of the item entering the country through a numerical sequence. The first 2 digits define the Chapter of the HTS, the next two define the heading, and the remaining digits of the numerical

⁷² UM APPS website: <https://umapps.miami.edu/signon.asp> Access request forms available at: <http://controller.miami.edu/accounting/forms/index.html>

⁷³<https://usitc.gov/tata/hts/index.htm>



string are subheadings. Therefore, it is essential to understand the specifics of the item being shipped. If you list, for example, an electric motor, your HTS code must correctly identify the characteristics of that motor.

Harmonized Tariff Schedule of the United States (2013) (Rev. 1)					
Annotated for Statistical Reporting Purposes					
Heading/ Subheading	Stat Suf- fix	Article Description	Unit of Quantity	Rates of Duty	
				1 General	2 Special
8501		Electric motors and generators (excluding generating sets):			
8501.10		Motors of an output not exceeding 37.5 W:			
		Of under 18.65 W:			
8501.10.20	00	Synchronous, valued not over \$4 each.....	No.....	6.7%	Free (A,AU,B,BH, CA,CL,CO,E,IL,J, JO,KR,MA,MX, OM,P,PA,PE,SG)
8501.10.40		Other.....		4.4%	Free (A,AU,B,BH, CA,CL,CO,E,IL,J, JO,KR,MA,MX, OM,P,PA,PE,SG)
	20	AC.....	No.		
	40	DC:			
	60	Brushless.....	No.		
	80	Other.....	No.		
8501.10.60		Of 18.65 W or more but not exceeding 37.5 W.....		2.8%	Free (A,AU,B,BH, CA,CL,CO,E,IL,J, JO,KR,MA,MX, OM,P,PA,PE,SG)
	20	AC.....	No.		
		DC:			

Screen shot of Chapter 85 of the U.S. Harmonized Tariff Schedule.

Other documentation may be required. Consult the freight forwarder or shipping agent for proper guidance.

12. INTERNATIONAL TRAVEL

Electronic devices used in day-to-day activities likely carry encryption technologies that are subject to restrictions imposed by the U.S. Government. Some of these devices include smartphones, tablets, or laptops. In most instances, there is not a problem in traveling with these devices. The biggest risk comes when travel is to a country that is sanctioned⁷⁴ by the U.S. Government. Traveling internationally with sensitive information such as unpublished research or confidential information may also violate regulations and/or award or contract terms.

Before traveling overseas....

1. Ask, "Do I absolutely, positively need to take the item(s)?"
2. If yes, verify that the country you are traveling to is not one that is sanctioned.
3. Consult with UM-IT about obtaining a 'loaner' device.
4. Contact the ECO for additional guidance.

In some cases, it may be possible to get a License Exception from UM's ECO which can be issued within a few business days.

12.1. TMP License Exception

When traveling, some items may qualify for use of the TMP License Exception⁷⁵, including use in International Waters. Items that could qualify for use of this exception would be UM-owned laptops, tablets, PDAs, smartphones, data storage devices, and encrypted software. This license exception is not available for equipment, components, or software designed for use in / by / with most satellites or spacecraft. The UM-owned item must return to the U.S. within 12 months and must remain in the effective control⁷⁶ and ownership of the authorized UM personnel for the duration of travel.

⁷⁴ List of restricted and embargoed countries posted by the U.S. Department of State. http://www.pmdtc.state.gov/embargoed_countries/index.html

⁷⁵ 15 CFR §740.9(a)(2)(i)

⁷⁶ "effective control" means retaining physical possession of an item or maintaining it in a secured environment.



Researchers may need to take other UM-owned equipment temporarily outside of the United States for use in UM research. Some equipment such as global positioning systems (GPS), thermal imaging cameras, inertial measurement units, and specialty software are highly restricted and may require an export license – even if one hand-carries the item, thus the TMP License Exception could not be used.

The TMP License Exception is only available to UM personnel for UM-owned devices when traveling on UM business.

12.2. License Exception BAG

License Exception BAG⁷⁷ (Baggage) is an exception that is available for personal devices. However, UM is not responsible for personal devices that UM personnel take during business travel. All UM business activities should be conducted on UM owned devices. You cannot use License Exception BAG for encryption items and software that is subject to controls, which usually carry an ECCN of 5x002. In addition, if the country of destination bans encryption technology from being imported, you will need to leave your device at home as the License Exception BAG will not be accepted. (Refer to the [section 7.1](#) above on encryption)

To obtain the forms for the License Exception TMP and License Exception BAG, please go to the “Office of Research Administration’s Export Control Compliance” web site listed below, select “Compliance Policies and Forms”, locate the TMP and BAG UM forms. The links to the TMP – EXPORT-F-005 and BAG EXPORT-F-008 forms are located in the SOP. www.miami.edu/exportcontrol

12.3. International SOS

[International SOS](#) is a security service available to all UM personnel and students for UM approved activities. International SOS helps the traveler with security alerts and threat forecasts, health advisories, security evacuation, and assistance if your passport is lost or stolen.

UM policy “[International Travel Approval & Authorization Form](#)” applies to all UM personnel who travel on behalf of and/or are reimbursed for travel expenses by UM regardless of funding source.

Travel to countries that appear on the U.S. Department of State [Travel Warning list](#) or [do not have formal diplomatic relations](#) requires the approval of the Provost or his/her designee. Once UM’s International Travel Authorization form is fully approved, the traveler must register with International SOS. UM personnel must include a copy of the approved International Travel Authorization Form **and** International SOS registration with their Business Expense Reimbursement Form (eBERF) in order to be recompensed.

12.4. “Clean” Devices

A “clean” device, such as a laptop, has no export-controlled hardware, software, data or information. It has no high-encryption software. It has no personal files or settings, no passwords, no student records, personnel records or other sensitive confidential information. It may contain commercially available software and encryption that protects any UM network log-in. Utilizing a “clean” device reduces the risk of loss, theft or inadvertent disclosure of protected information.

UM-IT will not disable any encryption currently installed on UM-owned devices as this voids the purpose of the encryption software. UM personnel who travel internationally may consult [UM-IT](#) for a loaner device to use while traveling on UM business.

Requesting a loaner device from UM-IT is ideal for UM personnel who are traveling to a country that prohibits encryption technology from entering and where License Exceptions BAG or TMP are not accepted.

⁷⁷ UM Personnel considering License Exception BAG should review [15 CFR §740.14](#) for details and consult the ECO in advance.



13. REPORTING

As with any business activity, recordkeeping practices are essential in maintaining accountability especially with respect to export-controlled transactions. Federal regulations define procedures that must be met in order to comply with recordkeeping practices for export controlled transactions. These regulations along with UM policy must be maintained by all UM personnel.

Any person having knowledge of a potential violation or noncompliance with the provisions of this policy or any export control directive shall immediately report the circumstances surrounding the activity to UM's ECO or file a report through UM's [Cane Watch](#) program. UM will investigate thoroughly and disclose involvement in violations to the proper authorities in accordance with applicable regulations.

13.1. Recordkeeping

Keeping logs and records of when technical data is released and defense services / technical assistance have been given is required by both the EAR⁷⁸ and ITAR.⁷⁹ ITAR requires a formal log to be maintained and it should contain the following information:

- Owner's Name (name of individual keeping the log)
- Applicable Export License/Agreement Number with approval date and expiration date
- Date of Export
- Name of Recipient
- Name & Country of Foreign Company
- How the item was exported
- Brief description of technical data
- ITAR or EAR Export Authorization
- Name & Initials of the person who released/exported the item

See [Appendix H](#) for template that may be used.

For the foreign person interchange and interaction recordkeeping form, please go to the "Office of Research Administration's Export Control Compliance" web site listed below, select "Compliance Policies and Forms", then scroll to "Travel" and select the link to "Export Control Recordkeeping Form" EXPORT-F-010. www.miami.edu/exportcontrol

You may "bundle" into a single entry or report: e-mails (which should be encrypted), phone calls, or faxes in a given week as long as the information exported are within the same scope.

You may not "bundle" actions of: mailing CDs, mailing hard copies of documents, posting information to a Program Tracking System (PTS) site, posting information to a File Transfer Protocol (FTP) site, posting information to an intranet site, providing foreign person access to database, sharing information with foreign visitors at UM campus – including UM foreign person employees, or information shared during a UM employee's travel to a foreign country.

Departments must keep copies of all documentation, including required licenses, financial records and shipping documentation such as invoices, Shippers Export Declarations (SEDs), Automated Export System (AES) records, and any internal campus forms related to export control regulations in their research project files for a period of five (5) years from the date of the export, re-export or controlled deemed export. A copy of such documentation must also be forwarded to UM's ECO who will maintain the records for the same period of time.

Export control files may contain controlled information and should be secured in a locked cabinet when not in use.

⁷⁸ [15 CFR §762.2-762.7](#)

⁷⁹ [22 CFR §123.22 and §123.26](#)



13.2. Cane Watch

UM is committed to the highest standards of ethical behavior as described in the [Business Conduct and Ethical Standards for Faculty and Staff handbook](#). UM is committed to an environment where open, honest communications are the expectation, not the exception. Employees should feel comfortable approaching their supervisor or manager to discuss instances where a violation of policies or standards may have occurred. In those situations where an employee prefers to make an anonymous report – via the web or by telephone – [‘Cane Watch](#) can be used to report concerns related to violations of policies and procedures, rules and regulations, or other irregularities / improprieties. UM employees who report an activity that may be in violation of a law, rule, or regulation are protected against retaliation by the [Whistleblower Protection Statement](#).

13.3. Audits

The ECO will conduct periodic reviews which may include inspections of equipment, work stations, storage and security documentation such as Technology Control Plans. UM personnel are to fully comply with requests and work to promptly resolve any discrepancies that may be found.

When an export control audit is being conducted by a federal agency or other governing authority, UM personnel are expected to respectfully comply with all reasonable requests. Unprofessional behavior by UM personnel will not be tolerated and will be handled in an appropriate manner by supervisors and UM leadership.⁸⁰

When a federal agent or other authorizing agency arrives at UM to conduct an export control audit, the employee with whom the auditor first makes contact is to:

1. Escort the auditor to an available conference room;
2. Notify immediate supervisor;
The supervisor will then:
3. Notify Dean / VCA / Department Chair;
4. Notify Export Compliance Director (305-284-9558);
The ECO will then:
5. Notify Executive Director of Compliance & Ethics (305-284-4657); and
6. Notify the General Counsel's Office (305-284-2700).

UM's ECD and the Executive Director of Compliance and Ethics will be the primary contact in working with the auditor⁸¹ in collecting responses and supporting materials from appropriate personnel with issues related to export compliance. All personnel are to adjust their schedules to be available throughout the duration of the audit.

14. TRAINING

Export compliance training is strongly encouraged for all UM personnel. However, this training is **MANDATORY** for UM employees who work with export controlled items and/or engage in research activities that are federally funded by certain agencies. UM personnel who are required to take the training will be identified by department administration and/or the ECO.

There are 2 live training sessions conducted regularly by the ECO. Employees may register for these sessions through [ULearn](#).

- o Export Compliance Basics
- o Export Compliance for Researchers

Depending on the type of research or activity being conducted, additional training may be required by other UM departments, such as:

⁸⁰ [VPR-P-001 "Disciplinary / Professional Conduct in the Course of Compliance"](#)

⁸¹ The Executive Director of Compliance & Ethics will always serve as the primary contact in working with auditors from any agency. The Executive Director of Compliance & Ethics should be contacted whenever notice of an audit is received.



- Disclosures & Conflict of Interest Management
- Environmental Health & Safety (EHS)
- Embryonic Stem Cell Research Oversight Committee (ESCRO) Support
- Institutional Animal Care and Use Committee (IACUC) Support
- Institutional Biosafety Committee (IBC) Support
- Office of Research Administration (ORA)
- Research Compliance & Quality Assurance (RCQA)
- Human Subjects Research Office (HSRO)
- Research Integrity

UM personnel should contact these departments directly for guidance on training that is appropriate for the research or activity being conducted.

14.1. Export Compliance Basics

“Export Compliance Basics” is a live training session conducted by UM’s ECO. This course is designed to provide a very high overview of export control issues and how they are related to UM business activities; provide resources and guidance for additional information. This course is especially beneficial for UM personnel involved in administrative functions including purchasing, contract negotiations, hiring of foreign persons, research, international travel, engineering, and security. All UM personnel are encouraged to attend.

14.2. Export Compliance for Researchers

“Export Compliance for Researchers” is a live training session conducted by the UM’s ECO. Successful completion of “Export Compliance Basics” training must be completed before enrolling in this course will be granted. This course is designed to provide a more in-depth overview of export control issues as they relate to research at UM, including but not limited to restricted party screening, restrictive clauses, purchasing of equipment, proposals, and technology control plans.

14.3. CITI Program

CITI Program⁸² is a subscription service providing research ethics education to all members of the research community. UM is a CITI participating organization.

The export control modules⁸³ offered through the CITI Program will not be accepted in lieu of the mandatory training outlined above; the CITI Program modules are optional supplemental information only.

14.4. Training Renewal

UM personnel who work with export controlled technologies and/or federally funded research will be required to retake training every two (2) years to ensure compliance with current U.S. export control laws and regulations.

15. TECHNOLOGY CONTROL PLANS

The purpose of the Technology Control Plan (TCP) is to identify the technology or technical data that may not be freely shared with employees, visitors, and students beyond that which has been approved. The TCP will also assist to identify activities that may pose additional restrictions, such as dissemination of classified, export controlled, restricted, confidential, and other proprietary items being utilized.

The TCP applies to all UM activities in which control or protection of items and/or work areas is necessary.⁸⁴ The procedures contained in the Technology Control Plan SOP ([EXPORT-S-003](#)) apply to all departments, colleges

⁸² CITI Program. (<http://www.citiprogram.org>)

⁸³ CITI Program Export Control modules were updated in 2014.

⁸⁴ [EXPORT-S-003](#): “SOP for Technology Control Plans”



and other units of the UM and pertain to all activities that are not specifically identified as Fundamental Research⁸⁵ and/or Educational Information⁸⁶ under relevant federal regulations.

Administration of the TCP will be the responsibility of the UM's ECO who will work with the PI to develop the TCP and apply for export license(s) where needed. Attending Export Compliance, live-training sessions will be required for all persons identified within the TCP. Renewal of training will be required biennially (every two years).

16. RETENTION POLICY

Records required to be maintained by export control laws and regulations will be kept for the longer of:

- (a) the record retention period required by the applicable export control regulations⁸⁷, or
- (b) the period required for retention of records as set forth in the [UM's record retention policy](#).

17. AUTHORIZING SIGNATURE

Print Name:	Barbara A. Cole	
Title:	Associate Vice President of Research Administration	
Signature		Date

18. DOCUMENT REVISION HISTORY

Description	Date	Author
Policy created and became effective	2014-Apr-01	Epley, Wendy M.
Policy updated, revised and became effective	2017 –July -21	Collins, William J.

19. APPENDICES

Appendix A: January 2013 Memo from VPR

Appendix B: Red Flag Identifiers

Appendix C: Export Compliance Decision Tree for Administration of Contract Provisions of Concern

Appendix D: Restrictive Clauses – Specific U.S. Government Access & Dissemination Controls

Appendix E: Export Compliance Review for Purchase Requisitions

Appendix F: Departmental Asset Inventory & Tracking Form

Appendix G: Export Compliance Decision Tree Shipping Items from the U.S.

Appendix H: Release of Technical Data Log

Appendix I: Export Compliance Decision Tree for International Visitors

Always use a form directly from the [Export Control Compliance website](#) to ensure the most current version is being used. Submittal of outdated forms may be returned.

⁸⁵ 15 CFR §734.8 "Information resulting from fundamental research"

⁸⁶ 15 CFR §734.9 "Education Information"

⁸⁷ 15 CFR §762 (EAR); 22 CFR §122.5, §123.22, and §123.25 (ITAR); and 31 CFR §501.601 (OFAC)



EXPORT MANAGEMENT & COMPLIANCE PROGRAM

APPENDIX - A

UNIVERSITY
OF MIAMI
OFFICE of RESEARCH



1400 NW 10th Avenue Ph: 305-243-7587
Dominion Tower, Suite 1205J-R64 Fax: 305-243-3549
Miami, Florida 33136 jlbixby@med.miami.edu

John L. Bixby, Ph.D.
Vice Provost for Research

DATE: January 3, 2013

TO: Deans, Department Chairs, Directors, Principal Investigators, Faculty and Staff

FROM: John L. Bixby, Ph.D., Vice Provost for Research

SUBJECT: University Policy Regarding U.S. Export Laws and Regulations

The University of Miami (UM) conducts focused research to advance knowledge, enhance student learning experiences, and build its reputation in the scientific and technical communities while providing positive returns on sponsoring partners' investments. While UM applies the principles of freedom of inquiry and open exchange of knowledge, we must also be mindful of the federal laws and regulations governing the exchange of research materials and results that are subject to export controls.

U.S. laws and regulations that govern export or access to certain information, technologies or financial services by foreign persons inside the U.S. have received increased attention and have affected programs at all major research universities. Although federal regulations restricting exports of goods and technologies have existed since the 1940's, these regulations have become more restrictive and their enforcement at universities has become more severe in recent years.

It is the policy of the University of Miami to comply with all U.S. export control laws and regulations, and to develop and maintain an export compliance program to enable UM employees, visiting scientists, postdoctoral fellows, students, and other persons retained by or working at or for UM to conduct their University business in accordance with these laws and regulations. No UM associate may engage in any activity that is prohibited by the U.S. Department of Commerce, the U.S. Department of State, the U.S. Department of Treasury's Office of Foreign Assets Control, or any other government agency with export governance. No University personnel may transfer any controlled item, including technology and technical data, without approved documentation from the appropriate governing agency.

It is unlawful under export control laws and regulations to send or take export controlled information out of the United States or to disclose, orally or visually, or transfer export controlled information to foreign nationals inside or outside the United States territory. The U.S. government defines exports to include not only tangible items such as biological materials, chemicals, and equipment, but also intangible information which may include research data, formulae, engineering designs and ideas. Furthermore, an export is defined not only as an actual physical shipment, but also includes electronic and voice transmissions. Exporting also includes the provision of training or services involving controlled equipment to foreign nationals in the U.S. or abroad, and engaging in transactions or providing services to entities and individuals who are on embargo or specially designated national lists.

Individuals as well as the University can be held criminally liable for violations of export control laws and regulations. Penalties are costly which can include monetary fines, imprisonment, deportation, loss of privileges, etc. Civil penalties can apply even to accidental or innocent violations.

If it is determined that export controlled items and/or information will be involved in the activities of the University of Miami, a Technology Control Plan (TCP) will be required. The Export Compliance Officer will work with the University department to implement a TCP to manage the receipt, creation, security and transfer of export controlled items.

It is the responsibility of each UM associate to secure their research and technology, chemicals and biological materials that they handle, and proprietary and Government articles or information entrusted against unauthorized use or theft.

Each UM associate is responsible for ensuring foreign persons, foreign entities, visitors, observers, outside service vendors, etc., have all been screened to confirm that the person or entity does not appear on any of the 200+ agency lists of denied / excluded parties. If your department is not set up with privileges to run screenings through the University approved RPS system, please contact the Export Compliance Officer for assistance.

Compliance with export controls must be considered and achieved *before* traveling, engaging in science or technology-based research, executing contracts or other agreements, purchasing high-technology devices or software, or engaging in any other activity that may be affected by export controls. In most cases, issues can be resolved quickly. In the few cases where an export license is required, this process can take up to as much as six (6) months or more – therefore it is wise to plan ahead. Contact the Export Compliance Officer as soon as possible.

The Office of Research Compliance under the direction of the Office of the Vice Provost for Research is responsible for helping the University community understand and comply with export control laws and regulations. Every UM associate is encouraged to attend Export Compliance training sessions which are regularly scheduled across all three (3) University campuses. (Gables, Medical, and RSMAS)

For additional information and tools to assist in determining if and how the regulations apply to your activity, as well as contact information for assistance with export control matters, please visit <http://www.miami.edu/exportcompliance>

This memo may also be viewed in PDF on the Export Control Compliance website "[Policies & Forms](#)" page.



APPENDIX - B



Red Flag Warnings



for International Partnerships and Export Compliance

If you find you or your department is involved with any of the following activities or situations, please contact the University's Export Compliance Officer immediately. These activities / situations may be subject to federal regulations which require further review.

- ✎ Contracts or agreements of any kind with restrictions on publication, exclusions or restrictions to foreign persons, and/or terms that contain export control statements.
- ✎ Non-Disclosure Agreements which note restrictions to exporting or foreign nationals
- ✎ Projects / Research which is for military purposes, whether its for developing, testing or providing a service of any kind.
- ✎ Sharing data or other information that is considered restricted, confidential or proprietary.
- ✎ Providing professional services to restricted persons or internationally
- ✎ Participating on a Dissertation Committee where student is a national from an embargoed country.
- ✎ Allowing students who are foreign nationals to work on research (regardless if they are paid or not)
- ✎ Collaborating or Partnering with foreigners, whether in the United States or abroad.
- ✎ Compensating foreign nationals from embargoed countries .
- ✎ Jointly shared laboratory equipment or technology that may be governed by dual-use regulations
- ✎ Visits / tours of labs or research by foreign persons. Including Observers and Visiting Scholars.
- ✎ Unsolicited email or other correspondence requesting visit of campuses / labs.
- ✎ Projects / Research using internal funding where Fundamental Research Exclusion is not applicable.
- ✎ Funding from Government agencies.
- ✎ Building of prototypes or models when funding is from a government agency.
- ✎ Using the knowledge or understanding gained from research that is directed toward the production of useful materials, devices, systems, or methods, including the design and development of prototypes and processes.
- ✎ Software that includes sharing source code, object code, and/or encryption technologies.
- ✎ Software that has restrictions to foreign nationals or export control statement in EULA.
- ✎ Drug testing on humans (FDA, 21 CFR 312.110)
- ✎ Purchasing or working with high-tech equipment such as high-energy lasers, sensors, acoustics, cryogenics, marine technologies, robots, transistors, any vehicle that is unmanned, radar, high performance computers, high-tech communications devices, wind tunnel aero-model technology, Nanotechnology and materials, microelectronics, advanced avionics and navigation, space-related technologies and prototypes, etc.
- ✎ Purchasing or working with select agents and/or toxins.
- ✎ Shipping technologies outside of the U.S. or deploying into international waters or air space.
- ✎ International shipping of pathogens.
- ✎ Traveling with unpublished research data or other proprietary/sensitive/controlled technologies or technical data. Includes blue prints, schematics, manuals, drawings, etc.
- ✎ Carrying technologies, including laptops, PDAs, GPS devices, etc. when traveling internationally to embargoed or restricted countries. *See the DoS countries list:* http://www.pmdtc.state.gov/embargoed_countries/index.html
- ✎ Traveling internationally to embargoed countries. (e.g., Cuba, China, Syria, Sudan, Iran, North Korea)



EXPORT MANAGEMENT & COMPLIANCE PROGRAM

APPENDIX – C

Export Compliance Decision Tree for Administration of Contract Provisions of Concern



**APPENDIX - D****** Restrictive Clauses ******Specific U.S. Government Access and Dissemination Controls**

Specific access and dissemination controls may be buried within the language of FARs, Defense Federal Acquisition Regulations (DFARs), and other agency-specific regulations included as part of a prime contract, or flowed down in a subcontract. These problematic clauses include, but are not limited to:

(a) FAR 52.227-14 (Rights in Data – General)

This clause grants the Government unlimited rights in data first produced or delivered under the contract. Government approval is required to assert copyright in data first produced in the performance of the contract and not published in academic, technical or professional journals, symposia proceedings, or similar works. For basic or applied research, suggest requesting Alternate IV to lift this restriction. Alternate IV provides the Contractor with the right to copyright data without Government permission.

(b) FAR 52.227-17 (Rights in Data – Special Works)

This clause prevents the release, distribution, and publication of any data originally produced in the performance of the award. This establishes controls for data generated by contractors for the Government's internal use and represents an absolute restriction on publication or dissemination of contractor-generated data. It should not apply to basic and applied research, and should be removed from the contract on the basis of exceptions to this clause's applicability. Refer to FAR 27.405(a)(1).

(c) DFAR 252.204-7000 (Disclosure of Information)

This clause states, "Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium, pertaining to any part of this contract or any program related to this contract." This is an example of a publication / information restriction that voids the FRE. Refer to 27.404(g)(2) & (3) and NSDD-189 as justification for getting the restriction removed. Also, you can refer to IRS Ruling 76-296. May also add alternate language that allows for review and comment on publications.

(d) DFAR 242.204-7008 (Export-Controlled Items)

This clause states, "The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR." The PI may be required to certify that the project does not involve any items that are subject to Export Control laws.

(e) ARL 52.004-4400 (Approval of Foreign Nationals)

All foreign persons must be approved before beginning work on the project. Contractor is required to divulge if any foreign persons will be working on the project. Provision of name, last country of residence, citizenship information, etc. is required. This clause is commonly found in contracts involving controlled technology and sponsored by military agencies. PI may be required to certify that no foreign persons will be working on the project. If no foreign persons will be employed on the project, Contractor may disregard this clause.

If the PI is doing basic research and the sponsor will take those results and work on the controlled technology at another location, you may be able to negotiate deleting this clause.

(f) ARL 52.005-4401 (Release of Information)

Includes reference to “non-releasable, unclassified information” and a requirement to “confer and consult” prior to release of information. It is unclear what the review entails. Therefore, the sponsor retains publication / information approval, which voids the FRE. Substitute with ARL Cooperative Agreement Language: Prior Review of Public Release, “The Parties agree to confer and consult with each other prior to publication or other disclosure of the results of work under this Agreement to ensure that no classified or proprietary information is released. Prior to submitting a manuscript for publication or before any other public disclosure, each Party will offer the other Party ample opportunity (not to exceed 60 days) to review such proposed publication or disclosure, to submit objections, and to file application letters for patents in a timely manner.”

(g) AFMC 5352.227-9000 (Requirement for ITAR License)

This clause requires an export license prior to assigning any foreign person to work on the project or allowing foreign persons access to the work, equipment, or technical data generated by the project. Foreign nationals make up a large portion of UM’s scientific undergraduate, graduate, post-doctoral, and visiting scholar population. Often, it is difficult to find qualified U.S. citizens to work on these projects. Also, many students depend on these projects to complete their thesis or dissertation. The PI needs to affirm if the project qualifies as basic or applied research. If it does, it may fall under an ITAR exclusion. Ask the Defense Project Manager if foreign students are allowed to work on the project. If yes, obtain confirmation in writing.

All UM personnel and students are to abide by Policy [“Contract Process”](#) which applies to any agreement that is legally enforceable between two or more parties which may also involve a commitment of UM funds, facilities, personnel, other resources in UM’s name, or a commitment for UM to give up a right it otherwise may have.

All contracts must be reviewed for business terms and conditions as defined in [“Contract Process”](#).



EXPORT MANAGEMENT & COMPLIANCE PROGRAM

APPENDIX - E

Export Compliance Review for Purchase Requisitions

The items listed below are examples of what would or would not require review by UM's ECO prior to issuance of a Purchase Order by the Purchasing Department. This list is not inclusive and merely serves as a guide.

Items that WOULD require a review	Items that WOULD NOT require a review
Biological select agents, toxins, pathogens, viruses	AED – Automated External Defibrillator
Cryogenic Devices	Ablation devices and accessories, radio frequency
HPCs – High Performance Computers	Animal Cages
High-Technology Communication Devices	Autoclaves
Inertial or Navigation Technologies	Blood management machines, auto transfusion
Lasers – DLIs, DF-CO2, Ion, Electron, etc.	Capnograph
Lenses – for radiation hardened TV cameras	Catheters – all types
Marine Technologies	Centrifuges – medical devices
Network Analyzers	External storage devices that do not have encryption technologies embedded into the hardware
Radar – tracking, airborne, altimeters, antennae, Inverse Synthetic Aperture (ISAR), laser, optical	Flow cytometry accessories, reagents and components
Robots	Incubators
Sensors – Angular rate, monospectral imaging, optical, direction finding, quartz, etc.	Manikin – medical training
Software with encryption technologies or access to source code	Medical supplies such as vaccines, bandages, gauze, needles, PPE, disinfectants, OTC medicines, etc.
Transistors – microwave, test equipment, S-parameter measurement	Monitors – multiparameter, cardiac, cardiopulmonary oxygenation systems, all patient types
Two dimensional focal plane arrays	Office supplies
Unmanned Aerial Vehicles (UAVs) – associated equipment, systems & components	Ophthalmology instruments (keratotome, reactors, speculums, etc.)
Uranium – natural or depleted, compounds & powders, titanium alloys, vapor products & tails collector systems, isotopes separation, lasers or laser systems, equipment & components	Parts and accessories for medical imaging devices (e.g., x-ray, ultrasound, CT or MRI scanners) that DO NOT contain nuclear or chemical compounds
Ventilated full or half (protective clothing) suits	Refrigerators – compartmental for morgues, standard commercial or residential grade.
Vessels – marine, positioning systems, austenitic stainless steel, marine systems or equipment	Service agreements or subscriptions
Waveform digitizers	Surgical instruments with no electronic components
Welders – MIG, E-beam, laser machines	Ultrasound machines and accessories
Wind tunnel aero-model technology	Ventilators – adult or infant/pediatric
Windows – glass for nuclear radiation shielding	
X-ray equipment – converters, generators, non-planar inspection equipment, projection image transfer	



For a more detailed listing of items that are controlled under the EAR, please refer to the [Commerce Control List](#). For items that are controlled under the ITAR, please refer to the [U.S. Munitions List](#).

APPENDIX - F

Departmental Asset Inventory & Tracking

Department Name:			
Department Location:		Campus:	
Department Property Administrator:		Contact Phone:	

Detailed Description:				
Date of Purchase:		Vendor:		
Quantity on Hand / Unit:		Value per Unit:	\$	Total Value: \$
Manufacturer:				
Model #		Serial / Lot #		
Export Classification:		Restricted to Foreign Nationals:		
Item Location / Stored:			Restricted Access:	
User(s) of item:				
Item Transferred to:			Transfer Date:	
Item Discarded (date):		Reason for Discard:		

Detailed Description:				
Date of Purchase:		Vendor:		
Quantity on Hand / Unit:		Value per Unit:	\$	Total Value: \$
Manufacturer:				
Model #		Serial / Lot #		
Export Classification:		Restricted to Foreign Nationals:		
Item Location / Stored:			Restricted Access:	
User(s) of item:				
Item Transferred to:			Transfer Date:	
Item Discarded (date):		Reason for Discard:		

Detailed Description:				
Date of Purchase:		Vendor:		
Quantity on Hand / Unit:		Value per Unit:	\$	Total Value: \$
Manufacturer:				
Model #		Serial / Lot #		
Export Classification:		Restricted to Foreign Nationals:		
Item Location / Stored:			Restricted Access:	
User(s) of item:				
Item Transferred to:			Transfer Date:	
Item Discarded (date):		Reason for Discard:		

Page ___ of ___

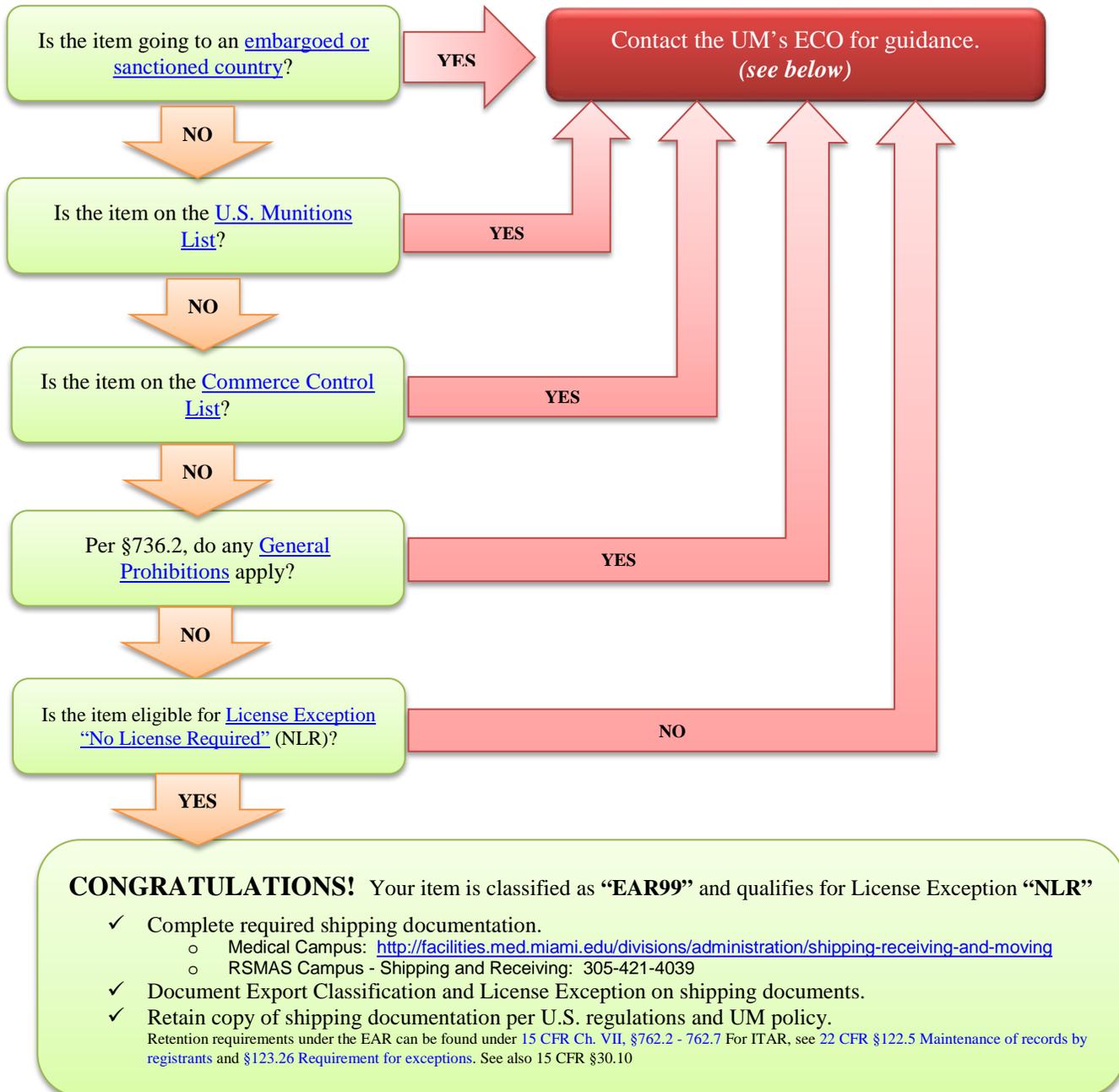
Date Items Inventoried: _____ By: _____
U.S. Government regulations and UM policy on retention is to be followed.



EXPORT MANAGEMENT & COMPLIANCE PROGRAM

APPENDIX - G

Decision-Making Tree (Simplified) for Shipping/Transporting Items Out of the U.S.



When contacting UM’s ECO, please have the following information available:

- Complete description of item
- Export Classification of item
 - You may contact the manufacturer/vendor directly to request this information. Use [EXPORT-F-002](#) which can be found on UM’s Export Compliance website.
- Country of Destination
- Name of Recipient / End-User of item
- Method of Transporting / Shipping



EXPORT MANAGEMENT & COMPLIANCE PROGRAM

APPENDIX - G

Export Compliance Decision Tree – Shipping Items from the U.S.

This form is to be used by the employee needing to assist in determining if an export license is required in order to ship items from the United States. For assistance please contact the [ECO](#).

Name of proposed recipient:	
Proposed destination country / national origin of proposed recipients:	

Checklist for export compliance for exports from the United States

I. CLASSIFICATION OF GOODS, TECHNOLOGY, TECHNICAL DATA AND SOFTWARE

Screening Question	Result
A Is the article, technical data or service to be provided subject to the International Traffic in Arms Regulations (ITAR)? (22 CFR §120) Any article, technical data or service that is specifically designed, developed, configured, adapted or modified for military or intelligence application, or for use in space, generally is subject to the ITAR. If it is subject to the ITAR, an export license from the U.S. Department of State will most likely be required. What is the classification number of the item per the U.S. Munitions List? This information can be obtained from the manufacturer/vendor. If your item is ITAR, you more than likely were asked to sign a form at the time of purchase identifying the item is ITAR and is bound by restrictions.	<input type="checkbox"/> Yes <input type="checkbox"/> No USML _____
B If not subject to the ITAR, are the goods, technology or software subject to the Export Administrations Regulations (EAR)? (15 CFR §734.2) What is the Export Control Classification Number (ECCN)? This information can be obtained from the manufacturer/vendor. You may also search for the item on the Commerce Control List (CCL), but if the manufacturer is still in business it is best to have them identify. Self-classifying items incorrectly can result in a violation of the Arms Export Control Act. The ECCN is an alphanumeric sequence. The ECCN is broken down by 10 categories (0-9), followed by 5 groups (A-E), and finally a set of 3-digits which identify the reason for control. Examples of an ECCN are 3A001, 7D994, 0A018. Items that do not appear in the CCL but are still controlled by the EAR fall into a "bucket" designation with a classification of "EAR99", provided that it is not controlled by another agency. Shipments of EAR99 items to an embargoed destination, denied persons, sanctioned entities or prohibited end-users or end-uses may require a license from the Bureau of Industry and Security.	<input type="checkbox"/> Yes <input type="checkbox"/> No ECCN _____

II. EAR LICENSE EXCEPTIONS / REQUIREMENTS

Once the EAR classification has been determined, the next step is to consult the "Country Chart" found at Supplement No. 1 to the EAR Part 738 and determine whether the License Requirements identified for the item apply to the country of ultimate destination. If the ECCN is controlled for export to the ultimate destination then a license is required unless a license exception can be applied.

PLEASE CONSULT WITH UM's ECO FOR ASSISTANCE WITH THIS SECTION

Screening Question	Result
A Is an export license required based on the ECCN for the material/technology and its destination? (See Supp. No. 1 to 15 CFR §774, Country Chart at Supp. No. 1 to 15 CFR §738)	<input type="checkbox"/> Yes <input type="checkbox"/> No
B Is a License Exception available? If so, are all the requirements for using it satisfied? (See ECCN for material / technology at issue, 15 CFR §740)	<input type="checkbox"/> Yes <input type="checkbox"/> No



III. RED FLAG, PROHIBITED PARTY AND PROHIBITED ACTIVITY REVIEW

Screening Question	Result
A Any knowledge of a prohibited nuclear end-use? (15 CFR §744.2)	<input type="checkbox"/> Yes <input type="checkbox"/> No
B Any knowledge of a prohibited missile technology end-use? (15 CFR § 744.3)	<input type="checkbox"/> Yes <input type="checkbox"/> No
C Any knowledge of a prohibited chemical or biological weapons end-use? (15 CFR § 744.4)	<input type="checkbox"/> Yes <input type="checkbox"/> No
D Any knowledge of a prohibited maritime nuclear propulsion end-use? (15 CFR §744.5)	<input type="checkbox"/> Yes <input type="checkbox"/> No
E Any reason to suspect involvement with terrorism or the financing or support of terrorism?	<input type="checkbox"/> Yes <input type="checkbox"/> No
F Any “Red Flags” raised by this transaction? (See Supp. No. 3 to 15 CFR §732 and the “Red Flags” attachment to this checklist)	<input type="checkbox"/> Yes <input type="checkbox"/> No
G Has any U.S. Government agency instructed you not to transact business with this person / entity?	<input type="checkbox"/> Yes <input type="checkbox"/> No
H Does the proposed recipient appear on any list of denied / restricted parties? (15 CFR §764) <i>Submit EXPORT-F-006 to request RPS</i>	<input type="checkbox"/> Yes <input type="checkbox"/> No
I Has any party to the transaction asked you to participate in an international boycott (such as an agreement to refuse to work with another person on the basis of race, religion, sex, national origin or nationality) or is the proposed recipient located in a country identified by the U.S. Department of Treasury as supporting boycotts?	<input type="checkbox"/> Yes <input type="checkbox"/> No

If yes, please complete the Anti-Boycott screen.

If you answered “YES” to any of the questions in this section, please explain.

IV. SHIPPING DETAILS

How is the item being shipped? (sea-freight, parcel-post, rail, etc.)	
Who is the freight forwarding company?	



Screening Question	
A	<p>Will a Shippers Export Declaration (SED) be filed or an exemption claimed and specified on the shipping documentation?</p> <p>This information is frequently found on the international air waybills for commercial shippers such as Federal Express, DHL, UPS, etc.</p>
	<input type="checkbox"/> Yes <input type="checkbox"/> No
B	<p>If the export is subject to the EAR and is on the CCL and thus <i>not</i> classified as EAR99, will the invoice on the bill of lading, air waybill, or other export control document that accompanies the shipment from its point of origin in the United States to the ultimate consignee or end-user abroad contain, at a minimum, the following requirement statement as required under 15 CFR §758.6?</p> <p><i>“These commodities, technology or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to U.S. law is prohibited.”</i></p>
	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
C	<p>If the export is subject to the ITAR, will the bill of lading, invoice and license include the following statements as required under 22 CFR §123.9(b)?</p> <p><i>“These commodities are authorized by the U.S. Government for export only to [country of ultimate destination] for use by [end-user]. They may not be transferred, transshipped on a non-continuous voyage, or otherwise disposed of in any other country, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of State.”</i></p>
	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
D	<p>If the transfer will be to a U.S. person, and UM will not be the exporter of record, is the documentation clear that the U.S. person is responsible for obtaining any necessary export authorization?</p>
	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p><i>If you answered “NO” to any of the questions in this section, please explain.</i></p>	

I attest that the information contained herein was completed honestly and I consulted the external resources for assistance to ensure the questions were answered appropriately. When needed I contacted the ECO for guidance.

Signature of UM Employee (Shipper):		Date:	
Name of UM Employee:		UM C#	
Title of UM Employee:			

PLEASE SUBMIT THIS FORM TO [UM's ECO](#) FOR REVIEW

*** THIS AREA FOR USE BY ECO ***	
<input type="checkbox"/> No License Required – OK to Export	<input type="checkbox"/> License Required Before Exporting Can Occur
Comments:	
Signature of ECD: William J. Collins	



APPENDIX - I

Export Compliance Decision Tree for International Visitors

