EXPORT COMPLIANCE PROCEDURE MANUAL

Latest Revision: 3/21/2022

Editorial Note: Consistent with the University Policy on Policies, all acronym definitions are designated at first usage by (“ ”). Words defined within the document are capitalized throughout the document.

Contents

I. Overview of Export Controls Regulations

A. Introduction

This Export Compliance Procedure Manual ("Manual") is designed to assist University of Louisiana at Lafayette ("University") faculty, administrators, staff, students, visitors, and individuals affiliated with the University by contract or otherwise (including, but not limited to, non-employees, such as vendors and independent contractors, volunteers, student organization advisors, and retirees) in complying with the University Export Control Policy and U.S. export controls. Persons contracting with the University may also be required to provide evidence of export control compliance, as necessary. Please refer to Appendix 4 herein and the University Export Control Policy for applicable definitions of key terms. If you have any questions regarding the material contained in this Manual, please contact the University's Office of Research Integrity ("ORI"), the Export Control Compliance Committee, and/or the Empowered Official:

- Director, Office of Research Integrity: Dr. Robin Broussard, robin.broussard@louisiana.edu, (337) 482-1419
- Chair, Export Control Compliance Committee: Prof. Chase Edwards, Associate Professor, Department of Economics and Finance, chase.edwards@louisiana.edu, (337) 482-6217
- Empowered Official: Dr. Ramesh Kolluru, Vice President for Research, Innovation, and Economic Development, ramesh.kolluru@louisiana.edu, (337) 482-6541

Export Control laws are a complex set of federal regulations designed to protect the interests of the United States ("U.S.") on a variety of fronts. Some regulated areas of research are obvious (*e.g.*, protecting national security by ensuring non-proliferation of weapon Technology). Other areas are less obvious. For example, we strive to protect U.S. economic competitiveness by ensuring that research funded by U.S. taxpayers is not distributed to unauthorized foreign entities. Export Control Laws govern how information, technologies, and commodities can be transmitted overseas to *anyone*, including U.S. citizens, or to foreign nationals in the U.S. In addition to controlling exports to countries or individuals who are citizens of or located in those countries, Export Control Laws ban exports to individuals and companies that have been involved in terrorist or drug trafficking activities as well as those who are barred from conducting exports because of previous violations of the Export Control Laws.

Several federal agencies have jurisdiction over the control of exports, including the U.S. Departments of Commerce, Energy, State, and Agriculture, and the Nuclear Regulatory Commission, and the U.S. Department of

Agriculture. The laws of the State of Louisiana governing the expenditure of state funds can also affect the transferability of intellectual property and other fruits of state-funded research.

Three agencies produce the bulk of Export Control Laws: the Department of State, which administers controls of defense exports through its Directorate of Defense Trade Controls ("DDTC"), the Department of Commerce, which administers export of commercial, 'dual-use' and less sensitive defense items and technologies through the Bureau of Industry and Security ("BIS"), and the Department of Treasury, which administers exports to Sanctioned and Embargoed countries and specially designated nationals through its Office of Foreign Asset Controls ("OFAC").

Navigating this maze of law and regulation is a complex endeavor that should not be undertaken without consultation with the ORI, the Export Control Compliance Committee, and the Empowered Official. Violations of these laws can have serious legal consequences. Failure to comply with the University Export Control Policy, the Procedures provided in this Manual, or to obtain appropriate licenses when necessary, may result in sanctions as described in the University Export Control Policy.

B. Export Control Laws at UL Lafayette

Export Control Laws apply to many activities at UL Lafayette that you might not expect. For example, entering into a contract with people listed on certain government lists or sending money to certain countries may require a license from the U.S. government. Shipping certain items, such as a robot for a student competition, carrying a thumb drive to an international conference, or even collaborating with a long-time co-author who has moved to an international university are all examples of relatively common tasks for University community members that might involve complying with Export Control Laws.

Institutions of higher education in the United States, including the University, have a long tradition of inventing and developing leading-edge technologies that are important for national security and economic competitiveness as well as for education and training scholars from around the world. In recognition of this role, the U.S. Departments of State and Commerce carve out special provisions in Export Control Laws whereby unrestricted research and classroom teaching activities at a university in the U.S. may be excluded from the regulations. Most research activities at the University will be Fundamental Research as defined in the University Export Control Policy and in Export Control Laws, and as a result, do not require an export "license" in most cases. Nonetheless, it is important to understand the limits on Fundamental Research in the context of the applicable Export Control Laws. Fundamental Research is further discussed in later sections of this Manual.

Much in the same way that the Internal Revenue Service places the burden of understanding and complying with tax law on the taxpayer, regardless of their sophistication or familiarity with the Tax Code, the U.S. export control agencies place the burden of understanding and complying with the regulations on the exporter.[1] Even though most research conducted at the University will not be subject to export control restrictions, it is important for the University community to be aware when activities potentially become controlled. The Export Control Laws may apply to research activities on campus if controlled equipment, data, or information is used in the conduct of that research. It is incumbent upon University researchers to verify what, if any, information is export controlled, and to prevent the dissemination of such information to foreign parties in the U.S. or abroad. This may be particularly challenging in the conduct of collaborative research with other institutions. The Export Control Laws apply to the export (even temporary) of controlled University owned equipment for field research and to the shipment of research materials or equipment to locations outside of the U.S., including using equipment on research vessels in international waters or vessels with Foreign Persons as crew members.

The following brief descriptions of Export Control Laws are meant to provide an overview of the regulations as they impact activities at the University. This is in no way a comprehensive list of all laws governing your work. Determining which, if any, of the regulations apply to a particular project is complex; the ORI will work closely with researchers to make that determination and, when necessary, seek a determination from the relevant agencies.

1. Department of State Regulations ("ITAR")

a. Regulatory Authority and Scope

The Arms Export Control Act ("AECA"), 22 U.S.C. § 2778 grants authority to the President of the United States to designate and control the export and import of Defense Articles and services. Presidential executive order 11958 delegates this responsibility to the Secretary of State. The Department of State Directorate of Defense Trade Controls ("DDTC") administers this authority through implementation of the International Traffic in Arms Regulations ("ITAR"), *22 C.F.R. §§ 120-130*. ITAR contains the United States Munitions List ("USML"), which includes Defense Articles and related Technical Data that are controlled for export purposes. In addition to the Defense Article or related Technical Data, constituent parts and components of the Defense Article are controlled under ITAR. For example, military aircraft are on the USML, as are their engines, electronic controls, and inertial navigation systems, even though such components may have other applications. If a commodity contains a part or component that is controlled under ITAR, such as a controlled inertial navigation system, then that commodity is also controlled under ITAR, regardless of whether or not that commodity has an inherently military purpose. Thus, an autopilot system used in basic robotics research at the University may be controlled under ITAR.

[1] See GAO Report "Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities:", December 2006, available at *http://www.gao.gov/assets/260/254189.pdf.*

Many items designed for military use are also used for research completely unrelated to that military use. These specific items are controlled under ITAR even though they are not being used in any military activity. It is important to understand that ITAR designation is unrelated to the University's use of a controlled item.

b. Important ITAR Definitions

In order to understand the requirements of ITAR it is important to understand terminology specific to the regulation such as Defense Article, Technical Data, and defense service.

Additionally, it is important to understand how ITAR defines Fundamental Research and Public Domain information. Additional definitions can be found in Appendix 4 of this Manual.

Defense Article is defined in the University Export Control Policy, as well as at *22.C.F.R. § 120.6*. A Defense Article is any item or technical data that was or will be specifically designed, developed, configured, adapted, or modified for a controlled use listed on the USML. In addition to the items on the USML, models or other items that reveal technical data related to USML items are also considered to be defense articles.

Technical Data is defined in the University Export Control Policy, as well as at *22.C.F.R. § 120.10*. Technical Data includes information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of Defense Articles. This information includes blueprints, drawings, photographs, plans, instructions and documentation. ITAR Technical Data also includes classified information relating to Defense Articles and Defense Services, information covered by an invention secrecy order and software directly related to Defense Articles.

Defense Service is defined in *22 C.F.R. § 120.9*. The definition includes furnishing of assistance, including training, to a Foreign Person, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of Defense Articles. It also includes providing any Foreign Person any Technical Data as defined above. It is important to note that Defense Services may apply even if the information being furnished is in the Public Domain.

Public Domain is defined in the University Export Control Policy, as well as at *22 C.F.R. § 120.11*. Public domain information is information that is published and generally accessible or available to the public. The ITAR describes means by which public domain information might be rightfully available, which in addition to libraries, subscriptions, newsstands and bookstores, include published patents and public release at conferences, meetings and trade shows **in** the United States where those venues are generally accessible to the public. Posting ITAR-controlled technical data to the Internet does not automatically make it public domain and may represent an illegal export.

Fundamental Research is defined in the University Export Control Policy, as well as at *22 CFR § 120.11(a)(8)*. It is basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research where the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. The ITAR considers Fundamental Research in science and engineering at accredited institutions of higher learning in the U.S. to be in the public domain, and, therefore, no export license would be needed to export the resulting information abroad or share it with foreign nationals in the United States. However, University research will not be considered Fundamental Research if: (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project activity, or (ii) the research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable. It is important to note that Fundamental Research applies only to the information generated, and not to any tangible technology created in the process.

c. The USML Categories

The USML defines twenty-one (21) classes of Defense Articles. For detailed descriptions of what is included in each category, please refer to *ITAR website*, ITAR Part 121 – the United States Munitions List. ITAR-controlled research at the University is typically included in Categories III, IV, VI, VIII, XII, XIV, and XV (highlighted in bold below). Note that Category XXI (Miscellaneous Articles) is reserved for future use by the DDTC for controlling new technologies that will fall under ITAR.

I. Firearms, Close Assault Weapons and Combat Shotguns

II. Guns and Armament

III. Ammunition/Ordinance

IV. Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines

V. Explosives, Propellants, Incendiary Agents, and their Constituents

VI. Vessels of War and Special Naval Equipment

VII. Tanks and Military Vehicles

VIII. Aircraft and Associated Equipment

IX. Military Training Equipment

X. Protective Personnel Equipment

XI. Military Electronics

XII. Fire Control, Range Finder, Optical and Guidance and Control Equipment

XIII. Auxiliary Military Equipment

XIV. Toxicological Agents and Equipment and Radiological Equipment

XV. Spacecraft Systems and Associated Equipment

XVI. Nuclear Weapons, Design and Testing Related Items

XVII. Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated

XVIII. Directed Energy Weapons

XIX. [Reserved]

XX. Submersible Vessels, Oceanographic and Associated Equipment

XXI. Miscellaneous Articles

d. Exporting Under ITAR

An export as defined under ITAR includes sending or taking a Defense Article out of the U.S., disclosing (including oral or visual disclosure) Technical Data to a Foreign Person whether in the U.S. or abroad, or performing a defense service on behalf of a Foreign Person whether in the U.S. or abroad. (See *22 C.F.R. § 120.17* for a complete description of export under ITAR).

This definition is extremely broad. It includes taking controlled Technical Data out of the U.S. on a laptop computer, smartphone, or USB drive, regardless of whether or not that information is viewed or accessed while abroad. It also includes allowing a Foreign Person to view or use a Defense Article in the U.S. Most exports of Defense Articles and Defense Services must be licensed by DDTC. Exports of ITAR controlled items are prohibited to some countries and individuals, meaning that an export license WILL NOT be granted. The list of proscribed destinations varies. University community members should consult the most up-to-date lists *on DDTC's Country Policies website* in consultation with the ORI.

e. Commodity Jurisdiction

DDTC has the authority to determine if an item or technology falls within the scope of ITAR or if the item/Technology is under the jurisdiction of the U.S. Department of Commerce for the purposes of export controls. While it is possible to self-classify an item, DDTC must be consulted if there is any doubt as to whether an article or service is subject to ITAR. At the University, the ORI will work with University community member(s) and the appropriate U.S. Government agencies to obtain correct classification for any University research project.

f. ITAR License Exemptions and Exclusions

While strict, ITAR has specific license exemptions which permit the permanent or temporary export of Defense Articles and Technical Data by U.S. Persons in lieu of obtaining an export license from DDTC. These exemptions are authorizations that cover very specific situations and have specific requirements. An important exemption to institutions of higher learning such as the University is the bona fide, full-time employee exemption[2] ("BFE"). The BFE allows for disclosure of unclassified Technical Data in the U.S. by U.S. institutions of higher learning to Foreign Persons who are bona fide and full-time regular employees of that institution. The BFE also requires that the foreign national has a permanent residence in the U.S. during the period of employment and is not a national of a country to which exports are prohibited. The term "bona fide and full-time regular employee" does not apply to student employees or post-docs. Most universities find that only H-1B visa holders meet the criteria of the exemption.

As previously discussed, a license is not needed to export information that is already found in the Public Domain. Information released in connection with catalog-listed courses at a university is excluded from ITAR export controls. This includes information released during lectures, instruction in teaching laboratories, and inclusion in course materials, as long as the information has already been rightfully published in the Public Domain. Additionally, information and Technology is not controlled if it is part of Fundamental Research.

2. Department of Commerce Regulations ("EAR")

a. Regulatory Authority and Scope

The *Export Administration Regulations* ("EAR") control the export of "dual use" items, which are items that have civilian uses, but which may also have military or other strategic applications. Common, real-life examples from the University include much of the cybersecurity research that is not included in ITAR, laboratory equipment such as centrifuges, signal analyzers and fabrication equipment (e.g., milling machines and etching equipment for electronics), as well as certain chemicals, ceramics, microorganisms, and toxins. These items are classified on the Commerce Control List ("CCL"). The CCL is a "positive list;" in other words, if an item is NOT listed on the CCL, then generally EAR does not apply.

Like ITAR, EAR includes a number of exceptions that are important to University researchers. These include exclusions for published information, information resulting from Fundamental Research, educational information,

[2] Full text of *§125.4(b)10.*

and the export or Reexport of items with less than de minimis U.S. content (where applicable). It is important to understand the definitions and limitations of each of these exclusions in order to correctly evaluate their applicability to specific activities. The ORI can assist in these interpretations.

b. Important EAR Definitions and Concepts

Export is defined in *15 C.F.R. § 734.13* as an actual shipment or transmission of items subject to EAR out of the U.S. as well as the release of Technology or software subject to EAR in a foreign country or to a foreign national either in the U.S. or abroad.

Deemed Export is defined in the University Export Control Policy, as well as at *15 C.F.R. § 734.13(a)(2)*. A deemed export is any release of technology or source code subject to the EAR to a foreign national, regardless of location. The release is deemed to be an export to the home country or countries of the foreign national. For the purposes of the EAR, legal U.S. permanent residents, naturalized citizens, and individuals protected under the Immigration and Naturalization Act (8 U.S.C. § 1324b(a)(3)), are not considered to be foreign nationals.

Reexport is defined in *15 C.F.R. § 734.14* as an actual shipment or transmission of items subject to EAR from one foreign country to another foreign country. For example, a research sample might be sent to collaborators in the United Kingdom, but then Reexported to researchers in Israel, a country with more significant export restrictions. Analysis of export licensing requirements must consider the final End-User, including any Reexports. It also means the release of Technology or software subject to EAR to a foreign national outside the U.S. ("**deemed Reexport**").

***De Minimis* U.S. content** is the amount of U.S. content, as determined by percentage of value of the U.S. content in the end item, required to make a foreign produced item subject to EAR. For some items, there is no *de minimis* content, meaning that any U.S. content will make the foreign-produced item controlled under EAR. For other items, the *de minimis* U.S. content for foreign produced items may be ten percent (10%) or twenty-five percent (25%) of the total value. See *15 C.F.R. § 734.4* for a complete discussion of the *de minimis* content rules.

Published Information and Software is defined in *15 C.F.R. § 734.7.* Information is published when it is accessible to the interested public in any form. Publications may take the form of periodicals, books, print, electronic media, public web sites, or any other media available for general distribution. It should be noted that published information and software under EAR differs from the ITAR in regarding most material subject to EAR to be publicly available once rightfully posted to a public website. Similarly, ITAR requires that information already be published to be considered in the Public Domain, whereas for EAR, information that has been, or is about to be published is considered published information.

General distribution may be defined as available to an interested community, such as a technical journal available to scientists in a relevant field, so long as the price charged for the publication does not exceed the cost of reproduction and distribution. Articles submitted to journals for consideration for publication are considered to be published, regardless of whether or not they are accepted. Published information also includes information readily available in libraries (including university libraries), as well as patents and published patent applications. Finally, release of information at a conference open to the participation of all technically qualified persons, is considered to be publication of that information.

Software is published when it is available for general distribution either free or at the cost of distribution. *However, strong encryption software remains controlled, regardless of general availability*.

Fundamental Research is basic and applied research in science and engineering, where the resulting information is intended to be published and shared broadly within the scientific community. Such research can be distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary reasons or specific national security reasons. The complete definition and discussion of Fundamental Research, including University based research is found at *15 C.F.R. § 734.8*. University research is considered to be fundamental to the extent that researchers do not accept restrictions on the publication of scientific and technical information resulting from the research. Temporary delays in publication for the protection of sponsor proprietary information do not remove research from the fundamental domain. However, if that sponsor's proprietary information is subject to EAR, then that information remains subject to the EAR during the conduct of the research and export licenses may be needed for non-US persons to utilize the proprietary information. **University researchers receiving proprietary information from corporate research sponsors should consult the Export Control Officer to ensure compliance with EAR in the conduct of the related research**. It is also important to note that Fundamental Research activities where non-U.S. persons need to use or access to export-controlled technology may require an export control license.

Educational information is referenced in *15 C.F.R. § 734.3(b)(3)(iii).* Educational information is information released as part of a course listed in the University's course catalog, and through instruction in the classroom or teaching laboratory. Participation in the course should be open to any qualified student enrolled at the academic institution. For example, participation by University international students in a University graduate course on design and manufacture of very high-speed integrated circuitry will not be subject to export controls, even though the Technology is on the CCL. The key factor is the fact that the information is provided by instruction in a catalog course. This applies to in person courses**. Courses delivered via internet for remote learning may have restrictions due to OFAC sanctions. Contact the ORI for assistance with online delivery, especially for graduate level STEM classes.**

As long as the course material is subject only to EAR (and not ITAR) and delivered face to face in the U.S., foreign students from any country may enroll in a course. Course activities are exempt from the controls, even if the course contains recent and unpublished results from laboratory research, so long as that research qualifies as Fundamental Research. (Note – students from foreign countries are required to adhere to the area of study as stated on their visa unless a change is granted. Depending on the type of visa, a student may not be allowed to change their major. Since people using the J-1 Exchange Visitor program cannot change their objective, J-1 students are not permitted to change academic majors in the U.S. F-1 students are permitted to change their majors. However, as an F-1 visa holder, you are responsible for maintaining an accurate, updated SEVIS I-20 as the major listed on the I-20 has implications for subsequent employment authorization. Students desiring to change their area of study must update the SEVIS record and obtain a new, accurate I-20 or DS-2019.)

c. The Commerce Control List

The Commerce Control List ("CCL") may be accessed on the *U.S. Department of Commerce website*. Items included on the CCL are assigned an export control classification number ("ECCN") based on a category and product group. There are ten (10) categories, numbered 0 – 9, and five (5) product groups, labeled A – E, within each category.

The category and product group generally describe the item being classified, and the remaining three (3) digits of the ECCN relate to the item specifications. An ECCN follows the nomenclature of "#α###", where the first "#" is the category, "α" is the product group, and "###" identifies the reason for control. As an example, an Unmanned Aerial Vehicle ("UAV") with the ability to maintain flight for thirty (30) to sixty (60) minutes has an ECCN of 9A012, where as an UAV with the capability of autonomous flight control has an ECCN of 9A120. In general, "###" with lower numbers are controlled to more destinations than those with higher numbers.

The categories and product groups are as follows:

Commerce Control List Categories	
0	Nuclear and Miscellaneous items
1	Materials, Chemicals, Microorganisms, and Toxins
2	Materials Processing
3	Electronics
4	Computers
5 (Part 1)	Telecommunications
5 (Part 2)	Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

Commerce Control List Product Groups	
A	Systems, equipment and components (finished or unfinished goods)
B	Test, inspection and production equipment (manufacturing equipment)
C	Material
D	Software
E	Technology

EAR export licensing regime is much more complex than that of ITAR. Under EAR, licensing requirements for export activities depend on what is being exported, the export destination, who will be using it, and what it will be used for. ECCN entries include a listing of the reasons for control that can be used in determining if an export license is necessary. While the most common controls are for anti-terrorism and national security, many other potential controls exist. The complete list of controls is found in *15 C.F.R. § 742*.

d. License Exceptions

While the CCL is much more extensive than the USML, many fewer licenses are required for items controlled under EAR than under ITAR. This is because of the many license exceptions that may be available for EAR controlled exports. It is important to understand that there are limitations on the use of license exceptions (see *15 C.F.R. § 740.2*), and that the use of a license exception may have an associated recordkeeping and notification requirement. More than one license exception may be available for a proposed activity. In such cases, the use of the exception with the fewest restrictions on use and least notification and recordkeeping requirements minimizes compliance burden. Members of the University community should consult with the ORI when making decisions as to the applicability of EAR license exceptions for proposed export activities.

A complete listing of EAR license exceptions may be found in *15 C.F.R. § 740*. Exceptions commonly applicable to members of the University community travelling abroad are “BAG”, which applies to personally-owned items taken abroad for personal use while abroad, and “TMP” which applies to the temporary export of University-owned equipment, including laptop computers and other equipment listed on the CCL, for work-related activities. These activities include professional presentations, teaching, and field research. It is important to note that there are limitations on the use of the TMP license exception; items must be returned to the U.S. within one (1) year of export, or if not returned, documentation of disposal is required. Items exported using the TMP license exception must be kept under the effective control of the traveler while abroad. Additionally, TMP is not applicable to some restricted locations, such as Cuba.

e. Commodity Classification

BIS encourages exporters to use the detailed descriptions in the CCL to identify the potential ECCN of items to be exported. However, in the event of an incorrect classification, the exporter is liable for any resulting violations of EAR and may be subject to penalties. Self-classification may be particularly difficult in the University environment where cutting edge-research pushes the boundaries of existing technologies, and in fact may not precisely meet the technical specifications as described in the existing CCL listings. Members of the University community who need assistance with classifying items should contact the ORI. When unsure about a self-classification, the University may submit the item/Technology to BIS for a formal classification. Please note that requests for classification by the BIS can take several months.

3. Anti-Boycott Restrictions

The Anti-Boycott provisions of EAR were designed to address foreign governments' boycotts of countries friendly to the U.S. The provisions were first implemented in response to the Arab League Boycott of Israel. Arab countries including Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen have been known to impose boycott restrictions on Israel and companies that do business with Israel. Companies, as well as individuals, are "blacklisted" under such boycotts.

The anti-boycott provisions are found in *15 C.F.R. § 760*. The provisions apply to any person or entity in the U.S. as well as to U.S. Persons or entities abroad and specifically prohibit the following activities:

- Agreement to refuse or actual refusing to do business with a boycotted country or with blacklisted persons;
- Agreement to discriminate or actual discrimination against other persons based on race, religion, sex, national origin, or nationality (e.g., agreeing to refuse to hire Israeli nationals);
- Providing information about race, religion, sex, or national origin of another person;
- Furnishing information about business relationships with boycotted countries or blacklisted persons (e.g., providing information about current or previous business in Israel);
- Furnishing information about membership concerning associations with charitable and fraternal organizations; or
- Paying or otherwise implementing letters of credit containing prohibited conditions or requirements.

Exceptions to these prohibitions exist but are very limited. See *15 CFR 760.3* for current exceptions. Additionally, U.S. Persons asked to engage in the prohibited activities are required to report the request to BIS. If you encounter any boycott language in a University activity or contract, please contact the ORI for assistance in determining whether an exception is applicable and if reporting to BIS is required.

4. Department of Treasury Regulations – Office of Foreign Asset Controls ("OFAC")

a. Regulatory Authority and Scope

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security interests. Many of the sanctions are based on United Nations and other international mandates. Sanctions are country/program specific and are subject to frequent change based on the changing geo-political landscape. In addition to foreign countries and regimes, OFAC imposes sanctions on individuals, such as people the U.S. government deems to be terrorists and narcotics traffickers. The implementing regulations for the OFAC sanctions are found in *31 C.F.R. §§ 500-599*, the Foreign Asset Control Regulations.

OFAC sanctions broadly prohibit most transactions between a U.S. Person and persons or entities in a Sanctioned and Embargoed Country or who have been declared specially designated nationals ("SDNs").

They prohibit importation and exportation of goods and services as well as related financial transactions or engaging in business activities with SDNs. As of early 2020, OFAC has sanctions against people or governments in countries including the Balkans, Belarus, Burundi, Burma/Myanmar, Central African Republic, Cuba, Democratic Republic of Congo, Iran, Iraq, Lebanon, Libya, Mali, Nicaragua, North Korea, Russia, Somalia, South Sudan, Sudan and Darfur, Syria, Ukraine, Venezuela, and Zimbabwe. Additional activity-based sanctions programs include Counter Narcotics Trafficking, Counter Terrorism, Non-Proliferation, and Transnational Criminal Organizations sanctions as well as the Rough Diamond Trade Controls. The activity-based sanctions programs are implemented through the designation of individuals engaging in the banned activities as SDNs. Updated lists of sanctioned countries are available on the *U.S. Department of Treasury website*.

b. OFAC Licensing for Country Based Programs

It is important to review the specific sanctions program before conducting activities with an OFAC-sanctioned entity or person, or in an OFAC-sanctioned country. The individual sanctions specifically describe what activities are exempt from the embargo (e.g., personal communications, exchange of informational materials, etc.) as well as what activities may be permitted under either a general or specific license. Activities that are permitted under a general license do not require specific permission from OFAC prior to engaging in the activity; however, the conditions of a general license must be carefully reviewed by the ORI, and the use of the general license documented. Activities that do not fall under an available general license may be eligible for a specific license from OFAC. Specific license requests must be submitted by the Export Control Officer or Empowered Official, as appropriate, and approved by OFAC prior to engaging in the sanctioned activity. Activities conducted under both general and specific licenses are subject to OFAC audit, and records must be maintained for five (5) years after the conclusion of the activity by ORI. At the University, ORI should be contacted when considering any proposed OFAC sanctioned activities. Please note that license applications to OFAC require substantial advance planning, often taking six (6) months or more to be adjudicated by OFAC once submitted.

5. Additional Considerations

a. Records/Record Retention

ITAR, EAR, and OFAC regulations all stipulate record keeping requirements for regulated export activities. Under each of these sets of regulations, records must be retained for five (5) years after the completion of the activity by ORI and made available to the regulating authority upon request. Records that should be retained include all memoranda, notes, correspondence (including email), financial records, shipping documentation, as well as any other information related to the export activities. Additionally, when an EAR license exception or ITAR license exemption is used, additional records documenting the applicability of the exception/exemption may be required, and in some cases, there may be additional reporting requirements.

b. Labeling of Export Controlled Material

Export of items controlled under ITAR or EAR should be clearly marked as controlled, with the appropriate regulatory control cited. Any export requiring a license, as well as exports with a dollar value greater than Two Thousand Five Hundred U.S. Dollars ($2,500.00), must be entered into the Department of Census Automated Export System ("AES") by the Export Control Officer or ORI prior to the export of the item or information. While commercial freight forwarders will usually handle the AES entry, ORI is able to assist the University community for the export of items being hand-carried or Technical Data being mailed or electronically transmitted.

c. Penalties for Export Violations

Violation of Export Control Laws can result in both civil and criminal penalties including fines and imprisonment. Although there is a maximum amount for a civil or criminal penalty, the actual penalty is often multiplied by the number of unlicensed exports. For instance, if multiple unauthorized shipments of the same item to the same end user were completed, each individual shipment could potentially incur the maximum penalty. Even a single unauthorized export may result in multiple violations (e.g., export without a license, false representation on shipping documents, acting with knowledge of a violation, etc.). Maximum penalties for violations under OFAC, ITAR, and EAR are One Million U.S. Dollars ($1,000,000.00) and criminal prison sentences can be up to twenty (20) years for individuals engaging in the violations. Violation of the Export Control Laws may result in the loss of future export privileges (EAR) or even from debarment from participation in future federal contracts (ITAR).

In assessing penalties, regulatory agencies will consider mitigating factors. Mitigating factors include whether the disclosure of the violation was made voluntarily, whether the violation is an isolated incident or part of a pattern of continuing behavior, whether there was a compliance program in place at the time of the violations, whether steps were taken to improve the compliance program after the discovery of the violation and whether the violation was due to inadvertent action, mistake of fact, or a good faith misinterpretation of the laws.

Additionally, violation of the University's Export Control Policy may be subject to those sanctions referenced in Section VI of the Policy.

Anyone aware of a possible violation of the University's Export Control Policy and/or Export Control Laws at the University must bring the matter to the attention of ORI and the Empowered Official who will review the matter and work towards a corrective action. Most importantly, if there is a question as to whether an activity would be a violation of the University's Export Control Policy and/or Export Control Laws, the University community is required to consult with ORI prior to engaging in the activity.

II. UL Lafayette Export Control Procedures

A. Commitment to Export Control Compliance

The University is committed both to the preservation of academic freedom and to compliance with all applicable Export Control Laws. The vast majority of teaching and research activity at the University falls within one or more exemptions and exclusions from licensing requirements, but it is important to understand how the laws described in the first section of this Manual apply to University practices and procedures, as well as the corresponding compliance obligations.

The U.S. government defines exports to include not only tangible or "physical" items such as biological materials, chemicals, and equipment, but also intangible information that 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 out of the United States (e.g., email or a phone call to a colleague at a foreign institution or remotely accessing controlled documents while travelling internationally). Exports also include the release of Technology to foreign nationals within the U.S., 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 nationals lists.

As stated in Section I, exports are controlled by multiple federal agencies including ITAR, EAR, and OFAC. Each agency has its own procedures for enforcement, but violations of any of these regulations can result in significant institutional and/or personal penalties including fines of up to One Million U.S. Dollars ($1,000,000.00) per violation, incarceration for up to twenty (20) years, and/or the loss of future exporting privileges.

As stated, the University is committed to the preservation of academic freedom. However, the University recognizes its obligation to comply with the U.S. Export Control Laws. Fortunately, most, but not all, research activities on campus fall under the "Fundamental Research Exemption", which provides that basic and applied research activities NOT subject to publication or access restrictions will not be subject to export controls. Other exemptions apply to information shared in the conduct of teaching activities on campus in the U.S. as well as to information that is already publicly available. The export regulations are complex and continually changing, so it is important to consider each activity on an individual basis.

The University's Office of Research Integrity is responsible for helping the University community understand and comply with the Export Control Laws and apply for export licenses when necessary. Please contact ORI for additional information including analytical tools to assist you in determining if and how the regulations apply to an activity, as well as points of contact for assistance with export control matters.

B. Roles and Responsibilities for Export Controls at UL Lafayette

While it is the responsibility of senior University administrators to ensure the existence of adequate resources and management support to comply with the Export Control Laws and to resolve identified export control issues, the following roles focus on other key actors in export compliance at the University (see also Appendix I).

1. Empowered Official ("EO")

The Vice President for Research, Innovation, and Economic Development is the University's Empowered Official ("EO") who is charged with all EO responsibilities required by ITAR and BIS. The EO has the authority to represent the University before the export control regulators in matters related to registration, licensing, commodity jurisdiction, and classification requests, and voluntary or directed disclosures. While certain oversight functions may be delegated, only the EO may sign paperwork and bind the University in any proceeding before DDTC, BIS, OFAC, or any other government agency with regard to export control responsibilities. In addition, the EO is the individual authorized by the University to apply for licenses or other government authorization involving export-controlled activities.

The EO will also work with the Export Control Compliance Committee to review and provide feedback on the University's export controls compliance program. The Export Control Compliance Committee reviews relevant University policies and procedures and makes recommendations to facilitate research in adherence with federal regulations and best practices among peers. The Export Control Compliance Committee is comprised of representatives from the University research community and administration affected by Export Control Laws.

2. Export Control Officer ("ECO")

The Director of ORI will assume the duties of the Export Control Officer ("ECO") and will be the primary University employee charged with ensuring that research activities comply with export control requirements. The ECO collaborates with Export Control Compliance Committee in order to accomplish the following tasks:

- Identify areas at the University that are impacted by Export Control Laws;
- Develop procedures and other guidance to assist the University in remaining in compliance with Export Control Laws;
- Educate inventors, principal investigators ("PIs"), research centers, and academic units about Export Control Laws and procedures at the University;
- Coordinate with other University units such as Purchasing, Travel, International Programs, the Graduate School, Human Resources, and the various research centers regarding Export Control Laws and procedures at the University;

- Monitor and interpret export control legislation;

- Apply for export licenses, commodity jurisdiction and classification requests, and advisory opinions from the U.S. Government;

- Coordinate the investigation and reporting of export control noncompliance as required;

- Work with others to facilitate understanding and compliance with export controls;

- Assist researchers and offices at the University when research involves export-controlled equipment or information;

- Seek advice from legal counsel specializing in export control issues in analyzing and handling export control compliance issues;

- Assist PIs in developing Technology control plans for research involving export-controlled items or information to ensure compliance with Export Control Laws;

- Advise and assist with record keeping (i.e., retention of documentation) for export-controlled activities at the University; and

- Maintain the University's Export Control website.

3. Export Control Compliance Committee ("ECCC")

The ECCC is a group of individuals appointed by the Vice President for Research, Innovation and Economic Development. The ECCC represents the diversity of areas impacted by Export Control Laws. They assist the ECO and the EO in identifying training needs, identifying potential export control issues, and serve as local points of contact within their areas for questions related to export controls. Some members of the ECCC are trained and have access to software to perform restricted party screening. The ECCC meets with the ECO on a regular basis to discuss the needs of the program and how to best promote the export control compliance program at the University.

a. ECCC Charge:

- Examine high functioning export control programs at peer institutions and align the University program with best practices at aspirational peer institutions;

- Perform an export control risk assessment for the University and provide a report and a set of recommendations to the Vice President for Research, Innovation, and Economic Development at the end of each Spring semester;

- Review and implement the University's Export Control Policy and program for the University;

- Develop policies ensuring compliance with respect to mandatory reporting of all sources of research support, financial interests, and relevant affiliations, as well as steps reducing risk to IP security;

- Develop policies and procedures addressing the management and reporting of financial conflicts of interest in research conducted at the University;
- Develop and maintain guidelines to assist the faculty, staff, and students on the following topics:
    - International collaboration guidelines;
    - International travel guidelines; and
    - International visitors' guidelines;
- Identify and recommend training opportunities for the faculty, staff, and students on the following topics:
    - International collaboration in research;
    - International travel;
    - International shipping; and
    - International visitors.
- Review circumstances having export control implications and provide expert guidance, as and when requested.

b. Composition:

The ECCC shall include, but not be limited to, representation by the following:

- Director of Research Integrity
- Office of Operational Review
- Information Security Officer
- Dean of Graduate School or delegate
- Office of International Affairs
- Office of Purchasing Administrative and Finance Division
- Computer and Electrical Engineering
- Center for Critical Infrastructure and Cyber Security
- Mechanical Engineering

- Materials Research
- Office of Innovation Management
- Office of Research and Sponsored Programs
- Office of Sponsored Finance Administration and Compliance

4. Research Administrators

The administrators within the Office of Vice President for Research, Innovation, and Economic Development, Office of Research and Sponsored Programs ("ORSP"), Operational Review, and the Office of Sponsored Programs Administration Finance ("SPFAC") (collectively, "Research Administrators") work closely with the ECCC, Office of Research Integrity, and the principal investigators in order to process research-related contracts. Together with ECO, Research Administrators will:

- Provide assistance to PIs in reviewing terms of sponsored program agreements, material transfer agreements (MTA) and other non-monetary agreements to identify restrictions on publication and dissemination of research results and flag such restrictions in agency requests for proposals;
- Provide assistance to PIs in identifying international components of sponsored program agreements, identifying potential export control issues in the proposed international component;
- Communicate identified potential export control issues to the PI and ORI; and
- Communicate with ORI about any changes in awards that necessitate a re-review of the project for export controls.

5. Administrators

The University administrators, who assist University departments with purchasing items, scheduling travel and shipping items are expected to have a basic understanding of export controls. This will be accomplished via completion of Export Control training in CITI. University business administrators will assist in ensuring compliance with Export Control Laws by identifying potential export issues in the activities where they are asked to assist with paperwork and scheduling This may include reviewing invoices for statements that items may not be exported, ensuring that payments do not go to, or contracts are not entered into with, anyone on the then-current SDN list, and ensuring that international travel is compliant with applicable Export Control Laws. To accomplish these goals, administrators are expected to request assistance from the ECO in reviewing any such item in question. The ECO will assist administrators to determine if such activity is allowed or requires a license.

6. Principal Investigators ("PIs")

PIs have expert knowledge of the type of information and Technology involved in a research project or other University activity, such as presenting at conferences and discussing research findings with fellow researchers or collaborators. PIs must ensure that they do not disclose controlled information, such as information that has been provided to them under a corporate non-disclosure agreement, or transfer export-controlled articles or services to a foreign national without prior authorization as may be required. Each PI must:

- Understand his/her obligations under the Export Control Laws;
- Assist the ECO in correctly classifying Technology and items that are subject to Export Control Laws;
- Assist in developing and maintaining the conditions of a Technology Control Plan for any activity, data, or equipment where the need for such a plan is identified;
- Ensure that research staff and students have been trained on the Technology Control Plan and on the Export Control Laws, should any apply; and
- Notify the ECO and EO of any attempt by non-research project staff to obtain information or technology that is or may become export-controlled or has dual use potential.

C. Export Control Analysis Procedures

An export control analysis may occur when a PI submits a proposal, receives an award, desires to enter into an MOU, MTA, NDA, or non-monetary research agreement, changes the scope of an existing project, or instigates a solicitation (e.g., Request for Proposal ("RFP"), Invitation to Bid ("ITB"), Request for Quotation ("RFQ"), Solicitation for Offers ("SFO")).

ORSP, SPFAC, or Operational Review will send any proposal, contract, or award that is subject to Export Control Laws for review to the ECO. Purchasing may also request export control analysis from the ECO for purchases from foreign vendors. Travel may refer foreign travelers to the ECO for consultation, training, and licenses before foreign travel.

The University community may request training to identify export control red flags from ORI. The University subscribes to online training through the Collaborative Institutional Training Initiative ("CITI"). The ECO can also provide specific face-to-face training on topics as needed. Export control issues may exist when any of the following are found in documents, including but not limited to:

- References Export Control Laws;
- Restricts access or participation based on country of origin;

- Restricts the use of proprietary or confidential information;
- Grants the sponsor pre-publication review and approval for matters other than the inclusion of patent or sponsor proprietary/confidential information;
- Allows the sponsor to claim the results or data generated in the agreement as proprietary or trade secret;
- Involves export-controlled Technology, as identified in the contract;
- Includes foreign sponsors or collaborators;
- Travel, shipping, or work outside of the United States; and
- Military applications of project results.

If any export control concerns are identified, ORI is notified by ORSP, SPFAC, Operational Review, or Purchasing. During review, all persons and entities listed on contracts with export control items are screened against restricted party lists. Export controlled equipment, data, or technology is identified, and the appropriate compliance procedures are implemented.

D. Technology Control Plans (“TCP”) Procedures

Any University research project that involves export-controlled equipment or information, or has restrictions on access, requires a Technology Control Plan (“TCP”). The ECO will work with the PI to develop and implement a TCP to appropriately secure the equipment, data, or Technology from access by unlicensed non-U.S. Persons. Technology Control Plans shall address the following:

1. Project Personnel:

a. The PI is responsible for identifying in the TCP all persons who may have access to export controlled/restricted technology and software, and that such controlled Technical Data will not be disclosed, exported, or transferred in any manner not authorized under ITAR/EAR, unless a license specifically allowing the release is obtained.

b. The PI shall verify in the TCP that the University’s Office of Human Resources has confirmed the citizenship status of each project personnel granted access to such export-controlled materials by the PI.

c. PI will request assistance from ORI with obtaining licenses, as appropriate, for any personnel requiring access that are prohibited by Export Control Laws.

d. All personnel working with the Export Controlled Technology must sign the TCP.

e. Any new persons being added to the project to work with the Export Controlled Technology must also complete the required training and sign the TCP.

2. Training:

a. The PI shall verify in the TCP that each project personnel has completed the University's online export control training, including any additional modules pertaining to their type of project.

b. Each project personnel is required to attend a meeting with ORI where any questions arising out of the online training will be addressed.

3. Facilities:

a. The PI shall verify in the TCP that an access-controlled room will be used for storage of all export controlled physical materials (i.e., hardware, software, files, printed documentation) and that the room is clearly marked on the exterior door (i.e., signage) as a Restricted Area (e.g., "U.S. Persons only") and this approved TCP is posted clearly inside the room.

b. The PI shall verify in the TCP the method of controlling access to the access-controlled room. The process (room key or card) must be managed by the PI's department, and all access requests are made in writing by the PI. PI shall ensure that only approved personnel will be granted access. Review the available security options on the *IT Services - Security* website and make requests for electronic locks by emailing *psec@louisiana.edu*.

c. The PI shall verify in the TCP that regular custodial, recycling, and maintenance services are NOT to be provided in the access-controlled room and facilities management is given instructions that staff are not to access the room unaccompanied. PI shall ensure that project personnel are responsible for cleaning and/or escorting staff as visitors for occasional cleaning and maintenance services.

d. The PI shall confirm in the TCP that the access-controlled room has a shredder or disposal container for export controlled printed matter.

4. Visitor and Guest Access:

a. The PI shall verify in the TCP that all parties entering the access-controlled room who are not approved personnel will sign in and be accompanied by approved personnel. The University recommends that all visitors be approved by the PI prior to entering the facility. The PI will acknowledge in the TCP that Foreign Persons will not be allowed to enter the access-controlled room unless all export-controlled materials are secured in a locked cabinet or covered.

b. The PI shall confirm in the TCP that all sign in sheets must include the name of the guest/visitor, a confirmation of all parties' citizenship, a record of the responsible approved person chaperoning the visit, as well as the date of the visit.

5. Marking Documents and Hardware

a. The PI shall confirm in the TCP that all export restricted documents and hardware are to be clearly marked with "**WARNING** - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq.). Violations of these statutes are subject to severe criminal penalties."

6. Computer Access and Electronic Data

a. The PI shall verify in the TCP that all computers that store export-controlled materials must meet the minimum campus security standards. The campus minimum security standards require that the operating system is currently supported and patched, the computer is password protected and runs current virus protection software when available for the operating system, and host-based firewall is enabled to block inbound traffic. The IT Services office will validate the security of systems storing export-controlled data annually. A security review can typically be conducted within ten (10) business days.

b. The PI shall verify in the TCP that a secure system designated for use with export-controlled materials is used as the primary storage for all such materials. Export controlled data can be stored locally behind a firewall, on computers or networks requiring individual logins, encryption, regular security system checks and strong access controls. Alternatively, it can be stored in the cloud if it is unclassified, transferred using end-to-end encryption and cryptographically secured. The PI is responsible for ensuring that the system is secure. Individual departments may employ technology security staff that can assist with system security. The PI's department head shall be notified of the IP address and name of any system designated as export controlled. The department head will arrange additional monitoring for the server.

c. The PI shall verify in the TCP that the storage and backup of the export-controlled data is maintained in a secure facility on campus or stored on a password protected device that is clearly marked. No open remote storage of such documents is permitted (i.e., Dropbox or Google drive).

d. The PI shall acknowledge in the TCP that all export-controlled data and documents are required to be password protected. Supported data protection methods include PGP (for Windows and Mac) and TrueCrypt (for Linux). If it is not feasible to use PGP or Truecrypt, Microsoft Excel and Word 2010 or later may be used if the machine is physically secured and the password is not stored in publicly accessible location.

e. The PI shall verify in the TCP that access to University computers used for projects with export-controlled material is controlled by the PI or an information security professional appointed by the PI or the PI's department head and that only approved personnel will be granted access.

f. The PI shall verify in the TCP that remote access to these computers must use a secure connection (e.g., VPN, SSH, or similar).

g. The PI shall verify in the TCP that remotely working on export controlled restricted materials in public locations (e.g., coffee shops, airports, computer labs, etc.) is forbidden because the citizenship of onlookers cannot be verified.

h. The PI shall acknowledge in the TCP that transfer of export controlled restricted materials to remote storage like Dropbox or Google Drive is forbidden.

i. The PI shall acknowledge in the TCP that transfer of export-controlled materials to a laptop, personal computer, or portable drive (e.g., USB drive) by students or any research staff is forbidden.

j. The PI shall verify in the TCP that electronic transfer of export-controlled data and documents to the sponsor or approved project personnel shall use the sponsor-preferred system of delivery. All files and communication must include a statement notifying the recipient that the data is export controlled. ORI will provide the necessary language. A record/log of each transfer of technical data and date of transfer will be maintained.

7. Travel:

a. The PI shall acknowledge in the TCP that computers or any electronic devices, such as portable USB drives, containing export-controlled data cannot leave the U.S. without prior approval of ORI and receipt of licenses when necessary. Export licenses can take ninety (90) days or more from date of request to response. Requests for licenses are not guaranteed to be granted.

b. The PI shall further acknowledge in the TCP that project personnel travelling outside the United States with a laptop for conference presentation which may contain export-controlled materials are required to receive additional training. The ECO must be contacted thirty (30) days in advance of any anticipated international travel to ensure appropriate training.

8. Destruction:

a. The PI shall verify in the TCP how the export-controlled material(s) will be handled at the end of the project or when they are no longer needed (e.g., shredding, file wipes, destroy hard drive, return to sponsor, etc.).

E. Licensing Procedures

The ECO is responsible for coordinating, drafting, submitting, and managing any authorizing license for export-controlled activities. The PI must work with the ECO and the EO to ensure that the scope of the PI's project is covered by any such license. Any University personnel who is unsure about licensing requirements for proposed international activities or the use of controlled Technology by foreign nationals should consult the ECO six (6) months to one (1) year prior to engaging in the activity. Once a license is obtained, all provisos, conditions, and recordkeeping requirements must be met and maintained by the PI in coordination with Office of Research Integrity.

1. ITAR Licenses

Following an export control analysis of the project, the ECO may advise the PI, EO, and SPFAC that an ITAR license is needed. The ECO will draft a transmittal letter outlining the scope of the project. This letter is intended to explain the export-controlled aspects of the project to the licensing offices of the U.S. Department of State. This letter includes (but is not limited to) statement of work, proposed timeline of research, Technology to be exported, and projected foreign involvement or collaboration. The ECO then reviews the document with the PI to ensure all export-controlled portions of the statement of work are included. With authorization from the EO, the ECO will submit the appropriate DSP-5 form, transmittal letter, and any other relevant supplemental information to DDTC.

Upon DDTC approval, the ECO will review and advise the PI on the license provisos and will advise on implementation of a TCP and any recordkeeping requirements.

2. EAR Licenses

Following an export control analysis of the project, the ECO may advise the PI, EO, and SPFAC that an EAR license is required. The ECO drafts a letter of explanation that describes the scope of the project for the licensing officials of the U.S. Department of Commerce. The letter includes (but is not limited to) a statement of work, proposed timeline of project, list of export-controlled materials, and foreign national involvement or collaboration. The letter, appropriate BIS 748 form, and any additional supplementary information is submitted to BIS. Upon BIS approval, the ECO will review and advise the PI of any license conditions and will advise on the implementation of a TCP and any recordkeeping requirements.

3. OFAC Licenses

OFAC is unique in that while most activities with sanctioned countries may require licenses, some activities are authorized under OFAC "general" licenses and do not require prior approval by the United States government. As the name suggests, these general licenses apply to general activities with sanctioned countries. These activities include general travel (not tourism), general education and research activities, and other non-specific actions. However, any activity outside the scope of the available general license, such as activities that provide a service or any financial transaction, require a more specific license that can take six (6) months to one (1) year to obtain. If the PI anticipates any collaboration or activity with a sanctioned country, he or she will need to work closely with the ECO to obtain a specific OFAC license.

F. Training Procedures

Training is the foundation of a successful export compliance program, and the University is committed to providing and increasing awareness of export compliance across the University. The ECO, in collaboration with the ECCC, will prepare up-to-date training materials so that Employees or students engaged in export controls receive the appropriate preparation. The University's Export Control Policy requires export control compliance training for all research staff working on projects impacted by Export Control Laws (e.g., requiring an export license or government authorization to export). Such training is highly recommended for all researchers, especially those working with potentially export-controlled Technology.

The ECO strives to provide up-to-date guidance and online training materials. The ECO also provides face-to-face training when requested or necessary. The ECO also maintains records of training or briefings provided. In addition to in-person training sessions, training on export controls will be available online via the University's

Collaborative Institutional Training Initiative ("CITI") membership. Additional resources addressing special topics are available on the University's Export Control web page.

The ECCC will assist the ECO in implementing the export control training sessions or briefings relative to their respective schools, departments, centers, or institutes and business units. ECCC members will work with senior management as necessary to implement export training to fit the individual department needs.

G. Contract Procedures

In order to ensure the University's ability to meet the obligations of the Export Control Laws, Research Administrators will request that ORI review the contract and make a determination about whether the University is able to meet the requirements of the contract as it pertains to export control laws. ORI will gather information about the items to be used and disclosed during the period of the contract, as well as the persons who are involved. When necessary, the Office of Human Resources may be asked to verify whether an individual is a U.S. Person, or the individual's country of origin, or the individual's most recent residence. ORI will apply for export licenses or assist with TCP development as necessary based on the facts gathered during the contract review process. ORI will also assess the parties involved in the contract for denied/restricted party status (i.e., persons or entities who have been listed by the U.S. government as entities that cannot do business with U.S. people or entities).

H. Purchasing Procedures

For purchases identified as ITAR or EAR, the individuals submitting a purchase requisition are required to take the following steps to determine when to request the assistance from the ECO:

1. Is the item or Technology classified as ITAR?

   If yes, STOP and escalate to ECO.

   If no, continue purchase requisition.

2. Is the item classified under EAR such as when the vendor provides you with an Export Control Classification Number ("ECCN")?

   If yes, document the ECCN while proceeding with the purchasing requisition.

   Notify ECO of the ECCN.

   If the ECCN is EAR99, proceed with the purchase without notifying ECO

If no, contact the ECO for assistance.

3. For unusual situations such as the vendor insisting that their "standard terms" include unusual language, language preventing Reexport, or for any other unresolved concerns, contact the ECO.

I. Travel Procedures

When planning travel outside the U.S. for research or conferences, consult the ECO at least three (3) months prior to departure (some destinations may require six (6) months advance notice). Special considerations, training, or export licenses maybe needed for:

- Technology an individual would like to carry with them;
- Technology or equipment that an individual will ship to a foreign location;
- Plans for private conversations; or
- Emailing data or Technology while outside the U.S.

J. Shipping Procedures

Any individual shipping an item, including but not limited to biological materials, to a foreign country should consult with ORI six (6) months before shipping, if possible. The individual shall provide the following to ORI upon the initial consult:

- The item's name, manufacturer, and model number;
- The destination country, as well as any countries it may travel through to get to the destination;
- Expected length of time it will be in each country;
- Name of the end user(s);

ORI will perform an export analysis to determine any controls on the item based the item description, the countries involved, and the end user. If needed, ORI will assist the EO to apply for an export license for the item to be shipped. ORI will provide the shipper with the final assessment determination.

K. Recordkeeping Procedures

Export-related records shall be maintained for controlled items or activities. Unless otherwise provided for or instructed by the ECO in consultation with upper University administration and/or legal counsel, all records shall be maintained by ORI consistent with the University's record retention policy and shall be retained no less than five (5) years after the TCP termination date or license termination date, whichever is later.

If ITAR-controlled Technical Data are exported under an exemption, certain records of the transaction must be kept for five (5) years.[3] Such records include:

- A description of the unclassified Technical Data;
- The name of the recipient /End-User;
- The date / time of export;
- The method of transmission (*e.g.*, e-mail, fax, telephone, FedEx); and
- The exemption under which the export took place.

Note that information which meets the criteria of being in the Public Domain, being educational information, or resulting from Fundamental Research is not subject to export controls under ITAR. Therefore, the special requirement for recordkeeping when using an exclusion, exception, or exemption may not apply. However, it is a good practice to provide such description for each export to establish a record of compliance.

BIS has specific record-keeping requirements.[4] Generally, records required to be kept by EAR must be kept for a period of five (5) years from the last export date. However, if BIS or any other government agency makes a request for such records following a voluntary self-disclosure, the records must be maintained until the agency concerned provides written authorization otherwise.

L. Monitoring and Reporting Violations Procedures

In order to maintain the University's export compliance program and ensure consistent adherence to Export Control Laws, the ECO may conduct internal reviews of TCPs and certain projects; randomly or at the request of project personnel. The purpose of these reviews is to identify potential areas where violations of the University Export Control Policy and/or Export Control Laws may occur and assist researchers with additional controls and education to prevent violation. When a potential violation is identified, the University will consult legal counsel

[3] See 22 CFR *122.5* and *123.26*
[4] See *15 CFR 762.6*

to determine the appropriate steps to take. Since September 11, 2001, government agencies have dramatically increased the investigation in, and the successful prosecution of, export regulations violations. The penalties for these violations can be severe, including personal liability, monetary fines, and imprisonment. However, government agencies assign great weight to voluntary self-disclosures as a mitigating factor. It is University policy for any individual who suspects that a violation has occurred to immediately notify the ECO and the EO. Information will be gathered to determine if an actual violation occurred. All University Employees who act in good faith in reporting known or suspected violations of law or the University Export Control Policy are protected from retaliation to the extent of the law. If the reporter is the export controls violator, the U.S. government may choose to prosecute, depending on the severity of the offense. Additionally, any University Employee will be subject to disciplinary action if the Employee knowingly fabricated, distorted, or exaggerated the report.

Any individual who suspects a violation has occurred or has reason to believe that a person's actions may violate the Export Control Laws, purposely or inadvertently, must immediately notify the ECO and the EO. The report must contain:

- Date and time of the interaction;
- Type of interaction (e.g., email, face to face conversation);
- Name of person(s) making requests;
- Names of any witnesses to the interaction;
- Description of the research project involved; and
- Description of the information that was requested.

The ECO and the EO will gather information and work with legal counsel to determine the appropriate follow-up to the notification, which may include re-training on appropriate protective measures or a voluntary self-disclosure to the U.S. government. The EO may send an initial notification about the suspected violation to the appropriate government agency.[5] The EO, assisted by legal counsel and the ECO, will conduct an internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. Once the review is complete, the EO and ECO may provide the government agency with a supplementary letter containing a thorough narrative account of:

- The project's description and background;

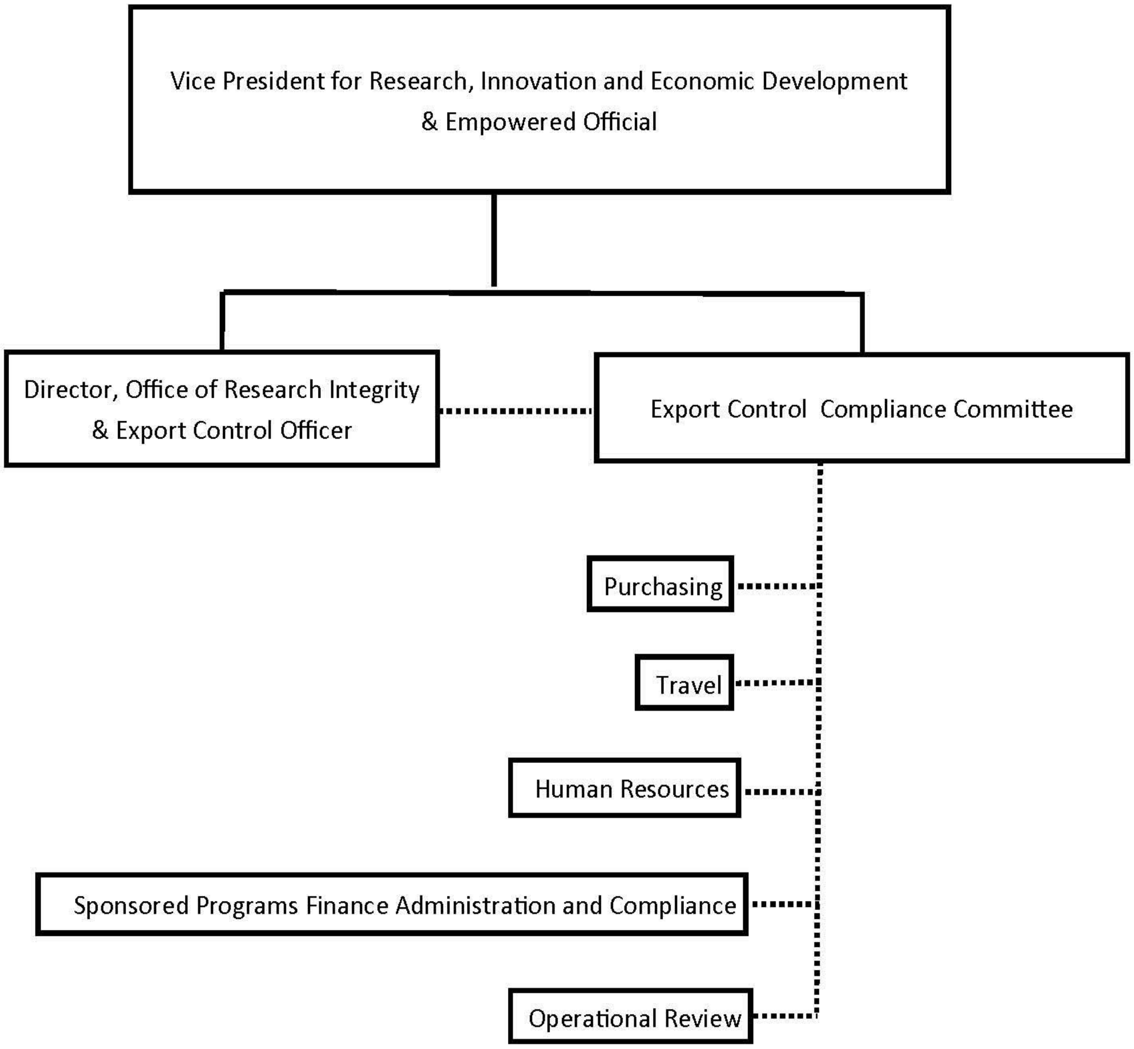
[5] For EAR violations, see *15 CFR 764.5*. For ITAR violations, *22 CFR 127.12(c)*.

- A description of the suspected violation;
- The items and controlled categories involved;
- The dates of the violations;
- The countries involved;
- The people involved and their citizenships;
- An explanation of why the alleged violation occurred;
- Any corrective actions taken; and
- The University’s commitment to export controls compliance.

Once the initial notification and supplementary letter have been sent, the University will follow the government agency’s instructions. Additionally, failure of Employees or students to comply with the University Export Control Policy or Export Control Laws may result in sanctions imposed by the University which may include, but not be limited to, disciplinary action up to termination of employment, as may be determined by the Provost or appropriate Vice President upon the recommendation of the EO in consultation with the Office of Human Resources or as may be determined by Student Rights and Responsibilities upon the recommendation of the EO.

III. Appendices

Appendix 1. University of Louisiana at Lafayette Export Controls Organization Chart


Vice President for Research, Innovation and Economic Development
& Empowered Official
Director, Office of Research Integrity
& Export Control Officer
Export Control Compliance Committee
Purchasing
Travel
Human Resources
Sponsored Programs Finance Administration and Compliance
Operational Review

Appendix 2. Export Control Review Forms

1. EXPORT CONTROL CHECKLIST

Use this checklist to determine if Export Control Laws may apply to your project.

Does this project or agreement:

	YES	NO
Restrict researcher participation (i.e., faculty, student, others) based on country of origin or citizenship?		
Require research participation in U.S.-citizen-only meetings?		
Grant the sponsor a right of prepublication review for matters other than the inclusion of patent and/or proprietary sponsor information?		
Provide that any part of the sponsoring, granting, or establishing documents may not be disclosed?		
Limit access to confidential data or involve a controlled technology?		
Involve research containing source code for encrypted software (other than publicly available software distributed at no charge)?		
Involve research, information, or software that could be used in the development of weapons of mass destruction (i.e., nuclear, biological, chemical), or their delivery systems?		
Involve equipment, software, services, or technology that is on the *United States Munitions List* ("USML").		
Involve equipment, software, services, or technology that is on the *Commerce Control List* ("CCL").		
Involve technical information or instructions concerning equipment, software, or technology on the USML or the CCL?		
Provide data, services or conduct any transaction with a sanctioned and embargoed country as defined by the *Office of Foreign Assets Control* ("OFAC")		

If the answer to any of the above questions is "yes," or other questions arise related to export controls, contact ORI at (337) 482-1419 or ori@louisiana.edu.

If accepting proprietary information is part of the project:

	YES	NO
Is the information clearly identified?		
Can the information be appropriately protected?		
Can proprietary information be removed from research results, so that results may be freely published?		

If the answer to any of the above questions about proprietary information is "no," please contact ORI at (337) 482-1419 or ori@louisiana.edu.

2. EXPORT LICENSE REVIEW WORKSHEET

PI Name: _____

Export Control Laws prohibit the unlicensed export of specific technologies for reasons of national security or protection of trade. If University research involves such specified technologies, the University may be required to obtain prior approval from the U.S. Departments of State, Commerce, or Treasury before allowing a) foreign nationals to participate in the research, b) partnering with a foreign company, or c) sharing research information—verbally or in writing—with people who are not U.S. citizens or permanent residents.

However, if you are doing “Fundamental Research” and the results will be in the “public domain” (see the University’s Export Control Policy for definitions), you may not have any export control issues unless you have a foreign national working with controlled (found on the Commerce Control List [CCL] or the U.S. Munitions List) proprietary Technology in conjunction with your research project.

In order to determine if an export license, TCP, or other formal agreement will be required for your activity, please provide the information requested below. The information will be used to classify your item and or activity to determine what restrictions may apply and to ensure that your collaborators, vendors, or end-users are not on any of the denied entities list maintained by the U.S. government.

1. Title of research project:

2. Funding source:

3. Statement of Work and attach a copy of the agreement (draft form is ok).

4. Are non-disclosure agreements necessary in furtherance of this research? If so, provide copies or sample copies. List items attached.

5. Provide names and affiliations of the parties involved in this activity (students, post docs, visiting scholars, collaborating organizations—list key principals from those organizations) and attach CVs for each person.

6. Research results. State what the item is, what it is a component of, what it does, how it works, and any

other information that explains the item that will be developed or tested in the course of the research project.

7. State what the item is originally designed for and why the item is being developed. State whether the item is being developed, designed, or modified specifically for military use, for commercial use, or both military and commercial use. Give examples of the uses for which it is being developed, designed, or modified. A brief product history is helpful.

8. Special Characteristics. State any military standards or military specification that the item is designed to meet. Describe any special characteristics of the item e.g., radiation-hardening, thermal or infrared signature reduction capability, and surveillance or intelligence gathering capability. If the item uses image intensification tubes, give the level of Technology (Gen II, Gen III, etc.).

9. Provide any other relevant information that would be helpful in making a commodity classification assessment. Include any brochure, specification sheet, marketing literature, Technical Data, IP disclosures, Patents or any other document that will assist in the determination.

10. In the course of the research activity, what are the item(s) (e.g., equipment, software, Technology, processes, commodities, etc.) that will be used or developed to conduct this research?

11. What are the processes involved?

    - Fabrication (i.e., briefly explain)?

    - What external facilities or vendors are involved?

    - What testing and/or simulation devices are you using?

    - What modeling software are you using? Is this proprietary software?

    - What and whose proprietary designs will you have access to?

- Who on the project team will have access to this proprietary information?

12. What equipment will be used or purchased in support of the research?

13. If items are to be purchased, list what countries the items will be purchased from.

14. How will the items (e.g., equipment, software, Technology, processes, commodities, etc.) be used by the team?

15. Will any non-U.S. Person (1) do ALL SIX of the following activities (or have access to information that would allow them to perform all six of the activities) with respect to the items: operation, installation (including on-site), maintenance, repair, overhaul, *and* refurbishing; OR (2) will any non-U.S. Person have access to its underlying manuals, blueprints, or Technology?

16. Is the information to be used or generated in this research publicly available OR is it being released to University students enrolled in a catalog-listed course or teaching lab?

17. Are the results of the research expected to be published?

18. If applicable, provide a short bibliography of publications related to this Technology.

Please send this completed form to Office of Research Integrity, ori@louisiana.edu, for review.

Appendix 3. Visiting Scholar Agreement

University of Louisiana at Lafayette

Visiting Scholar/Scientist Export Compliance Acknowledgement

This Visiting Scholar/Scientist Export Compliance Acknowledgment (the "Acknowledgement") includes information pertinent to the participation of visiting scholars/scientist in the University of Louisiana at Lafayette's ("UL Lafayette" or "University") export compliance program.

The University is committed to full compliance with all applicable U.S. laws and regulations, including those related to export control. Research and scholarly activities that are subject to U.S. export controls include the physical shipment or transmission of export-controlled items, software, materials, or Technical Data out of the U.S.; certain activities involving Defense Articles[1] or the provision of Defense Services[2]; release of controlled Technical Data, software, or source code to a foreign national or foreign government in the U.S. or abroad; involvement with restricted parties; and any activity involving a sanctioned country. Any activity, including informal discussion, directly related to the development, modification, manufacture, repair, testing, assessment, or deployment of military or defense equipment, systems, items, processes, software, or code is a defense service and may not be conducted at UL Lafayette without explicit authorization of the Empowered Official.

The University expects and requires all visiting scholars/scientists to abide by the University's Export Control Policy and U.S. laws and regulations, including those related to export control. In order to prevent inadvertent violation of U.S. export controls, visiting scholars/scientists are not permitted to participate in export controlled, proprietary, or confidential research programs without explicit authorization from the Empowered Official. UL Lafayette employees or students must not provide visiting scholars or scientists access to any information or technology that could be perceived as a providing a Defense Service without discussing with the Export Control Officer and receiving explicit prior authorization from the Empowered Official.

The University is committed to the free and open exchange of ideas outside of the scope of U.S. export control

[1] *Defense Article* means any item or Technical Data designated 22 CFR 121.1 (the U.S. Munitions List or "USML"); this includes most space-qualified hardware. The policy described in 22 CFR 121.3 is applicable to the designation of additional items. This term includes Technical Data recorded or stored in any physical form, models, mockups or other items that reveal Technical Data directly relating to items designated on the USML. It does not include basic marketing information on function or purpose or general system descriptions.

[2] *Defense Service* means (a) the furnishing of assistance (including training) to foreign persons, whether in the U.S. or abroad in the design, development, engineering, manufacturer, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; (b) the furnishing to foreign persons of any Technical Data controlled under 22 CFR 120.10 whether in the U.S. or abroad; or (c) military training of foreign units and forces, regular or irregular, including formal or informal instruction of foreign persons in the U.S. or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercises, and military advice.

regulations. Export controls do not apply to the conduct and reporting of basic and applied research, the results of which are typically published and shared broadly within the research community (often referred to as the Fundamental Research exclusion or exemption, or FRE). However, research results associated with research that does not qualify for the FRE must be protected as export controlled until they are authorized for unlimited public release or dissemination.

Signature

In signing this Acknowledgement, you agree that you have read this document in its entirety, understand the information provided within, and sign it voluntarily. You further understand that should you have questions related to the University Export Control Policy and/or U.S. export control regulations at any point during your time at UL Lafayette, you should contact UL Lafayette's Office of Research Integrity ((337) 482-1419; ori@louisiana.edu).

By signing below, you agree that you will not engage in export controlled, proprietary, or confidential work during your time at UL Lafayette without explicit authorization from the Empowered Official.

____

Printed Name

____ ____________________

Signature Date

Sponsoring Faculty Acknowledgement

I have read and understand the information provided on page one of this agreement. I understand that it is my responsibility to instruct the other members of my research or project team as necessary to prevent inadvertent violation of U.S. export control laws and regulations. I understand that should I have any questions related to U.S. export control regulations they should be directed to the UL Lafayette, Office of Research Integrity.

____

Sponsoring Faculty Printed Name

____ ____________________

Sponsoring Faculty Signature Date

Department Acknowledgement

Department Head Printed Name Title

Department Head Signature Date

Appendix 4. Technology Control Plan ("TCP") Template

PI(s):

Department:

Phone: **Email:**

Title of Project/Activity:

This TCP does not cover any materials classified higher than "Controlled Unclassified Information".

Technical Description of Export Controlled Material(s) to Be Received and/or Used:

Project Personnel & Citizenship:

Predetermined Export Classification: ECCN: **or ITAR Category:**

Date:

Project Personnel:

1. The PI is responsible for identifying all persons who may have access to ITAR/EAR restricted documentation and software, and that such controlled Technical Data will not be further disclosed, exported, or transferred in any manner not authorized under ITAR/EAR except with the prior written approval of the U.S. Department of State or the U.S. Department of Commerce, respectively.

2. UL Lafayette's Office of Human Resources is responsible for confirming the citizenship status of each Project Personnel granted access to the materials by the PI(s).

3. Screening Results of all Project Personnel Clear? Yes No

Training:

1. Each Project Personnel is required to complete the University of Louisiana at Lafayette online export control training, including any additional modules pertaining to their type of project.

2. Each Project Personnel is required to attend a meeting with the Office of Research Integrity ("ORI") where any questions arising out of the online training will be addressed.

3. Date Training Scheduled: ; Date Training Completed: ; Completed by:

   a. Project Personnel:

   b. Project Personnel:

   c. Project Personnel:

d. Project Personnel:

Licenses:

ORI and the Empowered Official must obtain licenses for any Foreign Person requiring access to an export-controlled project prior to the person receiving access to an export-controlled items or technology.

Individuals successfully completing the steps above are considered approved Project Personnel. Individuals may not receive restricted data or hardware until they are approved by the Export Control Officer and Empowered Official.

Facilities:

1. An ITAR/EAR designated room is used for storage of all ITAR/EAR controlled physical materials (i.e., hardware, software, files, printed documentation).

2. The ITAR/EAR room is clearly marked on the exterior door (ITAR/EAR Restricted Area (ITAR projects may designate U.S. Persons only)) and this approved TCP is posted clearly inside the room.

3. The ITAR/EAR room is access controlled. The access process (room key or card) is managed by the PI's department and all access requests are made in writing by the project PI. Only approved personnel will be granted access.

4. Regular custodial, recycling, and maintenance services are NOT to be provided in the ITAR/EAR room and facilities management is given instructions that staff are not to access the room unaccompanied. Project personnel are responsible for cleaning and/or escorting staff as visitors (as described below) for occasional cleaning and maintenance services.

5. The ITAR/EAR room must have a shredder or disposal container for export controlled printed matter.

6. Location (include building and room number(s), lab name, etc.):

Marking Documents and Hardware:

All ITAR restricted documents and hardware are to be clearly marked with "This document contains Technical Data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.). Violations of these export laws are subject to severe criminal penalties.

Visitor and Guest Access:

1. All parties entering the ITAR/EAR room who are not approved personnel must sign in and be accompanied by approved personnel. It is recommended that all visitors be approved by the PI prior to entering the facility. Foreign Persons will not be allowed to enter the access-controlled room unless all ITAR/EAR controlled materials are secured in a locked cabinet or covered.

2. Sign in sheets must include the name of the guest/visitor, a confirmation of all parties' citizenship, a record of the responsible approved person chaperoning the visit, as well as the date of the visit.

Computer Access and Electronic Data:

1. All computers that store ITAR/EAR materials must meet the minimum campus security standards. The campus minimum security standards require that the operating system is currently supported and patched, the computer is password protected and runs current virus protection software when available for the operating system, and host-based firewall is enabled to block inbound traffic. The IT Services office will validate the security of systems storing ITAR/EAR data annually. A security review can typically be conducted within one (1) business day.

2. A secure ITAR/EAR designated system is used as the primary storage for all ITAR/EAR materials. The PI or IT support personnel hired by the PI or PI's department is responsible for ensuring that the system is secure. The PI's department head shall be notified of the IP address and name of any ITAR/EAR designated system. The PI will arrange additional monitoring for the server.

3. Storage and backup of the ITAR/EAR system data is maintained in a secure facility on campus or stored on a password protected device that is clearly marked. No open remote storage of such documents is permitted (i.e., Dropbox or Google drive).

4. It is required that all ITAR/EAR data and documents be password protected. Supported data protection methods include PGP (for Windows and Mac) and TrueCrypt (for Linux). If it is not feasible to use PGP or Truecrypt, Microsoft Excel and Word 2010 or later may be used if the machine is physically secured and the password is not stored in publicly accessible location.

5. Access to UL Lafayette computers used for projects with ITAR/EAR-controlled material is managed by the PI or IT support personnel hired by the PI or PI's department. Only approved personnel will be granted access.

6. Remote access to these computers must use a secure connection (e.g., VPN, SSH, or similar).

7. Remotely working on ITAR/EAR restricted materials in public locations (e.g., coffee shops, airports, computer labs, etc.) is forbidden because the citizenship of onlookers cannot be verified.

8. Transfer of ITAR/EAR restricted materials to remote storage like Dropbox or Google Drive is forbidden.

9. Transfer of ITAR/EAR controlled materials to a laptop, personal computer, or portable drive (e.g., USB drive) is prohibited. If it is necessary to transfer ITAR/EAR data to such devices, a specific plan protecting the information must be clearly described, justified, approved by the ORI, and will only be granted for a specific period of time.

10. Electronic transfer of ITAR/EAR data and documents to the sponsor or approved project personnel shall use the sponsor-preferred system of delivery. All files and communication must include a statement notifying the recipient that the data is ITAR/EAR controlled. ORI will provide the necessary language. A record / log of each transfer of Technical Data and date of transfer will be maintained.

11. Please describe your security plans relative to computer access and electronic data:

Travel:

1. Computers or any electronic devices, such as portable USB drives, containing ITAR/EAR data cannot leave the United States without prior approval of ORI. It may be necessary to obtain an export license for such cases, which can take ninety (90) days or more.

2. Project Personnel travelling outside the United States with a laptop which may contain export-controlled materials are required to receive additional training. The Export Control Officer must be contacted thirty (30) days in advance of any anticipated international travel to ensure appropriate training. NOTE – If a license is necessary to carry the computer to the foreign country, thirty (30) days will not be enough time to obtain a license.

Destruction/Return of Materials:

Destruction or Return of Materials: Describe how the export-controlled material(s) will be handled at the end of the project or when they are not needed anymore (e.g., shredding, file wipes, destroy hard drive, return to sponsor, etc.).

PI SIGNATURE:

This is to acknowledge that I have read and understand the TCP for the stated project. I agree to update this TCP as required and as personnel are added to or deleted from this project.

PI Signature: ________________________________ Date: _____________________________

PROJECT PERSONNEL SIGNAUTRE(S):

This is to acknowledge that I have read and understand the TCP for the stated project. I have discussed the procedures with the PI and I agree to the follow all of the procedures contained in the TCP. If I have any questions about this TCP, its requirements, or following any procedure, I will contact the PI for advice before proceeding.

Signature: ___________________________________ Title ____________________________________

Printed Name: ________________________________ Date: ___________________________________

Signature: ___________________________________ Title ____________________________________

Printed Name: ________________________________ Date: ___________________________________

Signature: ___________________________________ Title ____________________________________

Printed Name: ________________________________ Date: ___________________________________

Appendix 5. Glossary

Commerce Control List ("CCL"): The CCL identifies specific item subject to the list-based controls of the Export Administration Regulations, under the export control jurisdiction of the Bureau of Industry and Security in the United States Department of Commerce (10 CFR § 774).

Defense Service: See Section I.B.1.b Important ITAR Definitions herein.

End-use, End-user: EAR controls the export of all items subject to EAR if they will be received by certain entities or used for certain purposes. Many EAR licenses and exemptions require certified "end use" statements from the receiver of EAR data or hardware.

Export Control Classification Number ("ECCN"): A five-character alphanumeric classification used under the EAR to identify items on the Commerce Control List.

Export Control Officer ("ECO"): – A person at the University who stays current on the Export Control Laws and assists faculty and staff with export control compliance and preparation of license applications.
At UL Lafayette, Director of ORI will be the ECO.

Foreign Person: The regulations define foreign person as anyone who is not a U.S. person. The EAR bases this on person's most recent citizenship or permanent residence. The ITAR bases this on the person's country of origin (i.e., country of birth) and all current citizenships.

Fundamental Research: See Section I.B.1.b Important ITAR Definitions or Section I.B.2.b Important EAR Definitions herein, as appropriate.

International Traffic In Arms Regulations ("ITAR"): The ITAR (22 CFR §120 – 130), under the jurisdiction of the United States Department of State, controls the export of articles, services, and related Technical Data whose most predominant application is that of defense. The Defense Articles, services, and Technical Data are listed on the USML.

Office of Foreign Assets Control ("OFAC"): An office within the United States Department of Treasury that administers and enforces economic embargoes and trade sanctions based on US foreign policy and national security goals.

Reexport: See Section I.B.2.b Important EAR Definitions –herein.

Restricted Parties: Individuals or entities with whom the university and its employees are prohibited by law, or require a license, to engage in export-controlled activities. Lists include Denied Parties List (OFAC), Debarred Parties List (ITAR) and Denied Persons List and Denied Entities List (EAR).

Restricted Research: University research, development, or testing subject to: publication restrictions, access or dissemination controls, or contract-specific national security restrictions (usually federally-funded). Restricted Research projects are subject to approval by ORI and may be subject to EAR and ITAR controls.

Sanctioned and Embargoed Countries: Countries designated by OFAC, ITAR, and EAR as having limited or comprehensive trade and arms sanctions imposed by the United States for reasons of anti-terrorism, non-proliferation, drug and human trafficking, human rights violations, and other reasons.

Specially Designated Nationals ("SDNs"): These are individuals or companies owned or controlled by, or acting for or on behalf of, targeted countries as listed by OFAC. These people and companies have their assets blocked and U.S. Persons are generally prohibited from dealing with them. The University performs restricted party screening to determine if a person or company is on one of the lists.

Technical Data: See Section I.B.1.b Important ITAR Definitions –herein.

Technology: In the EAR, technology is specific information necessary for the development, production, or use of a product.

United States Munitions List ("USML"): The USML includes articles, services, and related Technical Data designated as Defense Articles and services pursuant to ITAR.

US Person: For purposes of defense and dual-use exports, a U.S. person is defined as a U.S. entity or a U.S. citizen, or a person lawfully admitted for permanent residence in the United States (i.e., green card holder) A U.S. person may be engaged in activities that are export controlled, unless there are some additional restrictions that limit participation to U.S. citizens.

Appendix 6. Abbreviations

AECA	Arms Export Control Act
AES	Automated Export System
BIS	Department of Commerce - Bureau of Industry and Security
CCL	Commerce Control List

CFR	Code of Federal Regulations
CJ	Commodity Jurisdiction
DDTC	Department of State Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
EO	Empowered Official
ECO	Export Control Officer
ITAR	International Traffic in Arms Regulations
OFAC	Department of the Treasury Office of Foreign Assets Control
ORI	Office of Research Integrity
ORSP	Office of Research and Sponsored Programs
PI	Principal Investigator
SDN List	Specially Designated Nationals and Blocked Persons List
SPFAC	Sponsored Programs Finance Administration and Compliance
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List
VPN	Virtual Private Network