Florida State University
Export Controls Compliance Program Plan

(Updated 08/30/18)

NOTE: This Plan is a work-in-progress and will be updated as needed. In addition, the Federal government is currently undergoing a lengthy process to reform export control regulations. More information on this reform effort can be found at http://www.export.gov/ecr/.

The following information outlines how Florida State University (FSU) implements the core processes of its export compliance program. This Plan is intended to guide all affected personnel on managing export controlled transactions, and should be treated as a companion guide to FSU's Export Controls Policy and Federal regulations. Export Control definitions and commonly used phrases may be viewed here.

Questions about export controls should be addressed to Diana Key, Director, Office of Research Compliance Programs, at dkey@fsu.edu or (850) 644-8648 (hereinafter referred to as FSU's Export Controls Point of Contact or ECPOC).

SECTION 1 - Applicable U.S. Laws and Regulations

1.1 International Traffic in Arms Regulations

The Arms Export Control Act ("AECA"), implemented by the International Traffic in Arms Regulations ("ITAR") and administered by the State Department's Directorate of Defense Trade Controls prohibits the export and temporary import of defense articles and technical data, the manufacture abroad of defense articles using U.S. technology, the provision of defense services to foreign persons and the brokering of defense articles or services by all U.S. persons unless approved in advance by a DDTC-issued export license, agreement, or by qualification of an ITAR exemption. This includes the export of defense articles and defense services from the United States to any foreign destination or to any foreign person, whether located in the United States or abroad. The ITAR prohibits the export of all defense articles and services unless specifically permitted by the process described in the ITAR. ITAR controls are based on national security/nonproliferation and foreign policy considerations. There is considerable overlap among the policies underlying the ITAR and the Export Administration Regulations administered by the Commerce Department. Nevertheless, the objective of ITAR is to limit access to and use of "munitions" and related services and data— as opposed to dual-use items and technologies—to purposes and end-users that serve the foreign policy interests of the United States. As a result, the State Department is generally considered much less sensitive to commercial considerations than the Commerce Department.

Definitions important and specific to the ITAR include:

- A "defense item" is defined by the AECA at 22 U.S.C. 2778(j)(1)(4)(a) to mean defense articles, defense services and related technical data.
- A "defense article" means any item or technical data on the United States Munitions List ("USML"). Pursuant to the AECA at 11 U.S.C. 2794(s), defense articles include: (A) any weapon, weapon system, munition, aircraft, vessel, boat or other implement of war; (B) any property, installation, commodity, material, equipment, supply or goods used for the purpose of making military sales; (C) any machinery, facility, tool, material, supply, or other item necessary for the manufacture, production, processing, repair, servicing, storage, construction, transportation, operation, or use of any article listed in this paragraph; (D) any component or part of any article listed in this paragraph, but does not include merchant vessels,…source material,… byproduct material, special nuclear material, production facilities, utilization facilities, or atomic weapons or articles involving Restricted Data.

- A “defense service” means: (1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. (2) The furnishing to foreign persons of any technical data controlled under the ITAR. (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice, not defined as “assistance.”
- Technical Data means: (1) Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. (2) Classified information relating to defense articles and defense services; (3) Information covered by an invention secrecy order; (4) Software directly related to defense articles; (5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in the ITAR. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

U.S. Munitions List

The U.S. Munitions List (“USML”) is enumerated in 22 CFR Part 121 and specifies twenty-one (21) “Categories” of defense articles, with sub-itemization of “Significant Military Equipment” (SME) articles. SME is defined in 22 CFR § 120.7 as “articles for which special export controls are warranted because of their capacity for substantial military use or capability. An electronic version of the USML is available on the Department of State website at: http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/2013/ITAR_Part_121.pdf.

The twenty-one categories found on the USML are as follows:

Category I: Firearms, Close Assault Weapons and Combat Shotguns
Category II: Guns and Armament
Category III: Ammunition / Ordinance
Category IV: Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
Category V: Explosives and Energetic Materials, Propellants, Incendiary Agents and Their Constituents
Category VI: Surface Vessels of War and Special Naval Equipment
Category VII: Ground Vehicles
Category VIII: Aircraft and Related Articles
Category IX: Military Training Equipment and Training
Category X: Protective Personnel Equipment and Shelters
Category XI: Military Electronics
Category XII: Fire Control, Range Finder, Optical and Guidance and Control Equipment
Category XIII: Materials and Miscellaneous Articles
Category XIV: Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
Category XV: Spacecraft Systems and Associated Equipment

Category XVI: Nuclear Weapons, Design and Testing Related Items
Category XVII: Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
Category XVIII: Direct Energy Weapons
Category XIX: Gas Turbine Engines and Associated Equipment
Category XX: Submersible Vessels and Related Articles
Category XXI: Articles, Technical Data and Defense Services Not Otherwise Enumerated

Commodity Jurisdiction

The process of determining if an item, article, service, or technical data is on the USML and subject to the requirements of the ITAR is known as the "Commodity Jurisdiction" ("CJ") process. CJ is used by the U.S. Government if doubt exists as to whether an article or service is covered by the USML or some other regulations, such as the Commerce Control List ("CCL"). Designations of defense articles and defense services are made by the Department of State with the concurrence of the Department of Defense.

Proper CJ determination is absolutely essential to avoid violations because export compliance relies upon knowing which regulatory regime governs a particular export or activity (e.g., EAR or ITAR). The ITAR only regulates items, defense articles, services, and associated technical data of items specifically identified on the USML as opposed to other U.S. export regulations.

The order of review for CJ is to self-classify items, articles, or services to determine if they are subject to the ITAR by being listed on the USML, or if they meet the qualifications of being considered "specially designed". "Specially designed" is used to determine if an item or service meets the criteria of a defense article or defense service, or provides the equivalent performance capabilities of a defense article on the USML. If an article is not on the USML, or if it is not "specially designed" then it may be on the CCL, or subject to a different regulatory regime. The DDTC has a web-based interactive "Order of Review Decision Tool" to assist with this process:
http://www.pmddtc.state.gov/licensing/dt_OrderofReview.htm.

CJ is used to determine if an item or service meets the criteria of a defense article or defense service, or provides the equivalent performance capabilities of a defense article on the USML. The effort to determine whether an activity or item is subject to the ITAR (i.e., on the USML) is known as a "Jurisdictional Analysis", while the review for the EAR is known as "Commodity Classification." Conducting either of these analyses independent of government guidance is known as "self-classification."

The Jurisdictional Analysis process begins by reviewing the general characteristics of the item, technology, or proposed defense service. The general characteristics must fall within the proscribed requirements of "specially designed" to be subject to the ITAR. Commodities and software are "specially designed" if:

(1) As a result of development, has properties peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions described in the relevant U.S. Munitions List paragraph; or
(2) Is a part (see § 121.8(d) of this subchapter), component (see § 121.8(b) of this subchapter), accessory (see § 121.8(c) of this subchapter), attachment (see § 121.8(c) of this subchapter), or

software for use in or with a defense article.
(b) A part, component, accessory, attachment, or software is not controlled by a U.S. Munitions List ''catch-all'' or technical data control paragraph if it:
(1) Is subject to the EAR pursuant to a commodity jurisdiction determination;
(2) Is, regardless of form or fit, a fastener (e.g., screws, bolts, nuts, nut plates, studs, inserts, clips, rivets, pins), washer, spacer, insulator, grommet, bushing, spring, wire, or solder;
(3) Has the same function, performance capabilities, and the same or ''equivalent'' form and fit as a commodity or software used in or with a commodity that:
(i) Is or was in production (i.e., not in development); and
(ii) Is not enumerated on the U.S. Munitions List;
(4) Was or is being developed with knowledge that it is or would be for use in or with both defense articles enumerated on the U.S. Munitions List and also commodities not on the U.S. Munitions List; or
(5) Was or is being developed as a general purpose commodity or software.

If the technology meets the definitional requirements of qualifying as "specially designed" and is identified within a USML Category, the characteristics and functions of an article can be matched to a specific entry found on the USML.

DDTC has a web-based interactive "Specially Designed" decision tool to assist with this process: http://www.pmddtc.state.gov/licensing/dt_SpeciallyDesigned.htm.

Both the Departments of Commerce and State prefer for organizations to attempt to self-classify whenever possible; however, if a concluded jurisdictional determination cannot be made through either the Commodity Classification or Jurisdictional Analysis process, the U.S. Government will provide a definitive written determination in response to the submission of a "Commodity Jurisdiction Request." Necessary forms and processes are available at the DDTC website: http://www.pmddtc.state.gov/commodity_jurisdiction/index.html.

Definition of Export under the ITAR

The ITAR defines the term "export" broadly. The term applies not only to exports of tangible items from the U.S., but also to transfers of intangibles, such as technology or information. The ITAR defines as an "export" the passing of information or technology to foreign nationals even in the United States. The following are examples of exports:

1. Exports of articles from the U.S. territory:

- Shipping or taking a defense article out of the United States.
- Transferring title or ownership of a defense article to a foreign person, in or outside the United States.

2. Extra-territorial transfers:

- The re-export or re-transfer of defense articles from one foreign person to another, not previously authorized (i.e., transferring an article that has been exported to a foreign country from that country to a third country).

- Transferring the registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether the transfer occurs in the United States or abroad.

3. Export of intangibles:

- Disclosing technical data to a foreign person, whether in the United States or abroad, through oral, visual, or other means.
- Performing a defense service for a foreign person, whether in the United States or abroad.

Requirements for ITAR Export Authorization

Any person or entity who engages in the U.S. in the business of manufacturing or exporting or temporarily importing defense articles or furnishing defense services is required to register with the Department of State. Registration is a mandatory prerequisite to process license applications or invoke other approvals for an activity regulated by the ITAR, or invoke the use of an exemption to the license requirement. (See subsection 3.3, Empowered Officials) Once registered, licenses to export defense articles or perform defense services can be processed, including permanent and temporary export and import licenses and technical assistance agreements for complex programs for the provision of defense services. Certain licenses or exemptions or other government approvals are required to employ or allow foreign nationals to participate in activities subject to export requirements (see "deemed exports"). License applications or the invocation of other government approvals and exemptions contain additional certifications / transmittal letters, supporting documentation, and in some cases, non-transfer and use certification from the licensee and / or the foreign government of the licensee.

University research is subject to the ITAR when the research involves defense articles or technical data. Activities that involve defense articles or export-controlled technical data that involve foreign persons require a license or other government approval before the foreign person is permitted access to the articles or data. Instruction or methods involved in the ITAR-controlled research constitute the provisioning of "defense services", which is also a licensable activity. A "defense service" is equivalent to a "deemed export" under the EAR.

Proscribed Countries

Pursuant to U.S. policy related to arms embargoes, no ITAR exports, including license requests, exemptions and other government approvals for export may be made to countries proscribed in 22 C.F.R. § 126.1, such as China, Cuba, Iran, North Korea, Sudan, and Syria. Additional restrictions apply to other countries; a complete list of U.S. arms embargoes is available online at: http://www.pmddtc.state.gov/embargoed_countries/index.html.

1.2 Export Administration Regulations

The U.S. Department of Commerce's ("DoC") Bureau of Industry and Security ("BIS") regulates all dual-use technologies, materials, items, software, and technology not administered by another agency under the authority of the Export Administration Act of 1969 ("EAA") as enumerated in the Export Administration Regulations (EAR). The export control provisions of the EAR are intended to serve the national security, foreign policy, nonproliferation and short supply interests of the U.S., and in some cases, to carry out its international obligations. "Dual-use" items, products, technologies, and software

that have both military, or civilian and commercial applications, but were not "specially designed" for military applications are identified on the Commerce Control List ("CCL"). Certain technologies identified on the CCL may parallel those enumerated on the USML; however, the key distinguishing factor is the military application of the items.

All items of U.S.-origin, wherever located, are subject to the EAR. Foreign manufactured goods are generally exempt from the EAR re-export requirements if they contain less than a de minimis level of U.S. content by value. Such de minimis levels are set in the regulations relative to the ultimate destination of the export or re-export.

The EAR requires a license for the exportation of a wide range of items with potential "dual" commercial and military use, or otherwise of strategic value to the United States (but not made to military specifications). However, only items listed on the Commerce Control List ("CCL") require a license prior to exportation. Items not listed on the CCL are designated as EAR99 items and generally can be exported without a license, unless the export is to an embargoed country, or to a prohibited person or end-use.

Commerce Control List (CCL)

The EAR specifically enumerates controlled technologies on the CCL, including technical thresholds and performance parameters that distinguish various levels of controls. The CCL is divided into ten broad categories, which is further subdivided into five product groups. This scheme is the framework for a matrix-based system utilized within the EAR to categorize control, licensing, and exception requirements. Every commodity on the CCL is categorized according to an "Export Control Classification Number" ("ECCN"), which is a numeric-alpha code that describes the item and indicates licensing requirements. All ECCNs are listed within the CCL.

The following are the primary ten broad categories:

Category 0: Nuclear Materials, Facilities and Equipment & Miscellaneous
Category 1: Materials, Chemicals, Microorganisms and Toxins
Category 2: Material Processing
Category 3: Electronics
Category 4: Computers
Category 5: Telecommunications and Information Security
Category 6: Sensors and Lasers
Category 7: Navigation and Avionics
Category 8: Marine
Category 9: Propulsion Systems, Space Vehicles and Related Equipment

The following are the five product groups controlled under the EAR:

- Commodities, Equipment, Assemblies and Components. Finished or unfinished goods ranging from high-end microprocessors to airplanes, to ball bearings.
- Test, Inspection, Production and Manufacturing Equipment. This includes equipment specifically for manufacturing or testing controlled commodities, as well as certain generic machines, such as computer numerically controlled ("CNC") manufacturing and test equipment.
- Materials. This includes certain alloys and chemical compounds.

- Software. This includes software specifically associated with particular commodities or manufacturing equipment, as well as any software containing encryption and the applicable source code.
- Technology. Specific information necessary for the “development”, “production”, or “use” of a product. The information takes the form of “technical data” or “technical assistance”. Unlike the ITAR, there is generally no distinction between the two. However, the EAR may apply different standards to technology for “use” of a product than for the technology for the “design” or “manufacture” of the product.

Commodity Classification

As previously reviewed, the State Department’s CJ process is the primary means to determine which regulatory requirements are subject to an export activity. The State Department has jurisdiction to decide whether an item is ITAR- or EAR-controlled. DDTC encourages exporters to self-classify the product. If doubt exists, a CJ request may be submitted to DDTC to determine whether an item is ITAR- or EAR- controlled. Proper CJ determination is absolutely essential to avoid violations because export compliance relies upon knowing which regulatory regime governs the technology.

Once it is determined that an item is EAR-controlled, the exporter must determine its Export Control Classification Number (“ECCN”). The first digit identifies the general category within which the entry falls (e.g., 3A001). The letter immediately following this first digit identifies under which of the five groups the item is listed (e.g., 3 A001). The second digit differentiates individual entries by identifying the type of controls associated with the items contained in the entry (e.g., 3A001). Listed below are the Reasons for Control associated with this second digit.

Once the ECCN is determined all associated regulatory control requirements can be looked up using the Reasons for Control and Commerce Country Chart.

Reasons for Control

AT - Anti-Terrorism
CB - Chemical & Biological Weapons
CC - Crime Control
CW - Chemical Weapons Convention
EI - Encryption Items
FC - Firearms Convention
MT - Missile Technology
NS - National Security
NP - Nuclear Nonproliferation
RS - Regional Stability
SS - Short Supply
UN - United Nations Embargo
SI - Significant Items
SL - Surreptitious Listening

The reasons for controls identified on the ECCN are cross indexed to the "Commerce Country Chart" found in Supplement No. 1 to Part 738. The chart is available at: http://www.bis.doc.gov/index.php/forms-documents/doc_download/14-commerce-country-chart.

The "Country Chart" header identifies, for each applicable Reason for Control, a column name and number (e.g., CB Column 1). These column identifiers are used to direct you from the CCL to the appropriate column identifying the countries requiring a license. A license or other export authorization is required if the Chart and Reason for Control are marked with an X.

Requirements for EAR Export Authorization

Once determined that a license is required, an exporter can apply for export authorization from BIS.

The EAR contains a number of exceptions. Determining whether a particular exception applies requires review of the specific application as detailed in 15 C.F.R. § 740, as well as review of the notes on applicable license exceptions following the ECCN entry on the CCL. These exceptions include:

EAR License Exceptions

LVS - Items of limited value (value is set under each ECCN).
GBS - Items controlled for national security reasons to Group B countries.
CIV - Items controlled for national security reasons to particular countries where end-user is civilian.
TSR - Certain technology and software to certain countries.
APP - Computer exports to certain countries.
TMP - Certain temporary exports, re-exports, or imports, including items moving through the U.S. in transit.
RPL - Certain repair and replacement parts for items already exported.
GOV - Exports to certain government entities.
GFT - Certain gifts and humanitarian donations.
TSU - Certain mass-market technology and software.
BAG - Baggage exception.
AVS - Aircraft and vessels stopping in the U.S. and most exports of spare parts associated with aircraft and vessels.
APR - Allows re-export from certain countries.
ENC - Certain encryption devices and software.
AGR - Agricultural commodities.
CCD - Consumer communication devices
STA - Strategic Trade Authorization

Definition of Export under the EAR

The definition of export under the EAR is very broad, just as in the ITAR, and covers a broad range of products and activities. Definitions that are important and specific to the EAR include:

- **Export.** "Export" means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States.

- **Export of Technology or Software ("Deemed Export").** (i) Any release of technology or software subject to the EAR in a foreign country; or (ii) Any release of technology or source code subject to the EAR to a foreign national. Such release is deemed to be an export to the home country or countries of the foreign national. Deemed exports may occur through such means as a demonstration, oral briefing, or plant visit, as well as the electronic transmission of non-public data that will be received abroad.
- **Release of Technology or Software:** Technology or software is "released" for export through: (i) Visual inspection by foreign nationals of U.S.-origin equipment and facilities; (ii) Oral exchanges of information in the United States or abroad; or (iii) The application to situations abroad of personal knowledge or technical experience acquired in the United States.
- **Re-export.** "Re-export" means an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country; or release of technology or software subject to the EAR to a foreign national outside the United States, i.e., the shipment or transfer to a third country of goods or technology originally exported from the United States.
- **Re-export of Technology or Software (Deemed Re-export)**. Any release of technology or source code subject to the EAR to a foreign national of another country is a deemed re-export to the home country or countries of the foreign national. Re-export includes the export or re-export of items subject to the EAR that will transit through a country or countries or be transshipped in a country or countries to a new country or are intended for re-export to the new country, are deemed to be exports to the new country.

The release of technology or software source code to a foreign national in the United States is regulated, as is visual inspection by foreign nationals at U.S. facilities. This concept, as defined above, is considered a "deemed export."

The deemed export relies upon the transmission in the U.S. of technology as follows:

- **Technology**. Specific information necessary for the "development", "production", or "use" of a product. The information takes the form of "technical data" or "technical assistance". Unlike the ITAR, there is generally no distinction between the two. However, the EAR may apply different standards to technology for "use" of a product than for the technology for the "design" or "manufacture" of the product.
- **Required Information for the Development, Production, or Use of Items on the CCL:**
    - **Required.** As applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such "required" "technology" or "software" may be shared by different products.
    - **Development.** "Development" is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.
    - **Production.** Means all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance.
    - **Use.** Operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing**.**
    - **Technical Assistance.** Technical assistance—May take forms such as instruction, skills training, working knowledge, consulting services. "Technical assistance" may involve transfer of "technical data".

- **Technical Data.** May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memory.

1.3 Foreign Assets Control Regulations (FACR)

In addition to ITAR and EAR export restrictions, the Office of Foreign Assets Control ("OFAC") in the Treasury Department administers and enforces economic and trade sanctions against targeted:

Foreign governments (e.g. Iran, Sudan, Cuba)
Individuals (e.g. terrorists, narcotics traffickers)
Entities (e.g. drug front companies, charities linked to terrorist groups)
Practices (e.g. trade in rough diamonds, proliferation of WMDs)

There are three types of sanctions programs: (1) Comprehensive Sanctions, (2) Regime-Based Programs, and (3) Limited Programs.

Numerous publications and legislation encompass the spectrum of sanctions, embargoes, and financial regulations. Sanctions typically regulate:

- Transactions involving designated foreign countries or their nationals;
- Transactions with respect to securities registered or inscribed in the name of a designated national;
- Importation of and dealings in certain merchandise; and
- Holding certain types of blocked property in interest-bearing accounts.
- Transactions with specific entities or individuals known as "specially designated nationals," found in the Specially Designated Nationals List ("SDNL").

In many cases a general or specific license from OFAC is required in order to travel to sanctioned countries, or have transactions with sanctioned countries, entities, or individuals. University personnel will not engage in international collaborations with sanctioned countries, entities, or individuals without first consulting with FSU's Office of Research Compliance Programs to determine if an OFAC license is required.

1.4 Anti-Boycott Restrictions

U.S. anti-boycott policies proscribe certain actions regarding the Arab League's boycott of Israel and require reporting to the Department of Commerce or the Internal Revenue Service for certain boycott related communications or identification of participation in an international boycott. U.S. anti-boycott laws require U.S. firms and persons to refuse to participate in foreign boycotts that the U.S. government does not sanction. Any interaction, contracts, or agreements with foreign companies, entities and governmental agencies of identified participating boycott countries may require scrutiny to ensure there are no reportable boycott issues.

Prohibited conduct includes:

- Agreements to refuse or actual refusal to do business with or in Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality.
- Agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies.
- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person.
- Implementing letters of credit containing prohibited boycott terms or conditions.

Examples Include:

- Prohibited Boycott Condition in a Purchase Order:

"In the case of overseas suppliers, this order is placed subject to the suppliers being not on the Israel boycott list published by the central Arab League."

- Reportable boycott condition in an importer's purchase order:

"Goods of Israeli origin not acceptable."

- Prohibited Condition in a Contract

"The Contractor shall comply in all respects with the requirements of the laws of the State of Bahrain relating to the boycott of Israel. Goods manufactured by companies blacklisted by the Arab Boycott of Israel Office may not be imported into the State of Bahrain and must not be supplied against this Contract."

- Prohibited Boycott Condition in a Questionnaire

"1. Do you have or ever have had a branch or main company, factory or assembly plant in Israel or have sold to an Israeli?"

"2. Do you have or ever have had general agencies or offices in Israel for your Middle Eastern or international operations?"

- Prohibited Condition in a Trademark Application

"Requirement for the registration of pharmaceutical companies: Certification letter regarding the boycott of Israel (i.e., do not comprise any parts, raw materials, labor or capital of Israeli origin)."

1.5 Penalties for Export Violations

Penalties for export violations can apply to individuals and the university.

International Traffic in-Arms Regulations (ITAR)

Maximum $1,000,000 per violation or imprisonment of up to twenty years, or both pursuant to 22 U.S.C. 2778(c)

Export Administration Regulations (EAR)

- Criminal: Maximum $1,000,000 per violation or imprisonment of up to twenty years, or both
- Administrative: Maximum $11,000 per violation or $120,000 per violation for items involving national security
- Pursuant to the International Emergency Economic Powers (IEEPA) Enhancement Act:
    - Criminal: Maximum $100,000 per violation or imprisonment of up to twenty years, or both
    - Administrative: Maximum of greater of $250,000 per violation or twice the amount of the transaction

Office of Foreign Assets Control (OFAC)

Pursuant to the Trading with the Enemy Act (TEWA) of 1917, 50 USCS Sec 5

- Criminal (Willful Violation): Maximum $1,000,000 per violation, and up to $100,000 in individual fines, per violation or imprisonment of up to ten years, or both
- Criminal (Knowing Violation): Maximum $100,000 or up to ten years in prison, or both, per violation
- Civil: Maximum of $65,000 per violation

Pursuant to the International Emergency Economic Powers (IEEPA) Act, 20 USCS Sec 1701

- Criminal: Maximum $1,000,000 per violation or imprisonment of up to twenty years, or both
- Civil: Maximum $250,000 per violation, or twice the amount of the transaction

Administrative Penalties

- **Warning Letter:** are administrative determinations that a violation has occurred, but that a "good faith effort" (mitigating factor) to comply with the law and to cooperate with an investigation has been shown with no aggravating factors.
- **Denial Order / Interim Suspension:** deny the sanctioned party any U.S. export privileges and any access to U.S.-origin goods and technology, from any source, for a specified period of time or indefinitely and may be narrow in scope, such as a restriction on the export of specific items or to specific destinations.
- **Seizure & Forfeiture:** Commodities or technical data which have been, are being, or are intended to be exported or shipped from or taken out of the U.S. in violation of the Export Administration Act (EAA) or International Traffic in Arms Regulations (ITAR) are subject to being seized and forfeited including, the vehicles carrying such commodities or technical data.
- **Debarment:** includes the exclusion from practice or the denial of export privileges, including the revocation of contracts, loss of funding, debarment from government contracts or implementation of additional compliance measures.

1.6 Licensing

If a project is export-controlled and a license is needed for any purpose, only an Empowered Official may apply for the export license. Also, a Technology Control Plan, as described in Section 5, must be implemented. The ED Contact, in consultation with the Vice President for Research as needed, will prepare and sign the necessary documentation for obtaining a license.

1.7 Voluntary Self-Disclosure of Suspected Violations

Because of the complexity of the ITAR, EAR and FACR, accidental or inadvertent violations of export control regulations are possible. In research, a university may presumably discover that a researcher or collaborator has violated export control regulations. DDTC, BIS, and OFAC all have voluntary disclosure programs and procedures whereby a potential export violation may be self-disclosed. Specifically, Section 127.13 of the ITAR states that the DDTC:

Strongly encourages the disclosure of information…by persons, firms or any organization that believes they may have violated any export control provision of the Arms Export Control Act, or any regulations, order, license, or other authorization issued under the authority of the Arms Export Control Act.

The cognizant export administration agency may consider a voluntary disclosure as a mitigating factor in determining whether to impose any penalties (including monetary penalties) or seek other enforcement action. A failure to submit a Voluntary Self-Disclosure ("VSD") may be considered as an aggravating factor, likely increasing the penalties levied upon an organization.

FSU will report all potential violations of the ITAR, EAR, and FACR immediately upon discovery. A comprehensive report must be provided to the cognizant federal agency within 60 calendar days of the initial notification. A formal request for extension will be lodged with the appropriate agency if 60 days is insufficient. The procedure for detecting, investigating, reporting, and correcting suspected export violations are as follows:

The investigation of suspected export violations will be expedited. An investigation is a prerequisite to properly evaluate whether to submit a voluntary self-disclosure. All investigations will be carried out by an Empowered Official and reported to upper management. An investigation will examine the full scope of any potential violations, to include:

- Potential violation, causes, important facts, aggravating or mitigating circumstances.
- Parties involved, dates, places, locations, methods, export jurisdictions, means by which the violation was detected, type of export violation (physical, visual, oral, electronic);
- Short term corrective actions / stops implemented upon violation discovery, including parties involved in the corrective actions.

Investigation will consist of three phases:

1. Data preservation
a. Notify necessary parties of the investigation
b. Require parties to preserve all materials related to the subject matter
c. Categorize and review the types of information and documents relevant to the investigation

d. Demand strict compliance with data preservation
e. Inform parties of how information should be preserved
f. Designate a Point of Contact

2. Data collection and review
a. Document preservation and collection interviews
b. Collection and review of paper and electronic data

3. Interviews of relevant employees / participants
a. Following collection, review and organization of data, interviews with all relevant parties will be conducted.
b. A formal memo and summary of all interviews will be prepared.

Upon conclusion of data collection, interviews and evaluation, a formal report will be prepared. Facts developed during the course of the investigation are important for VSD purposes in addition to university decision-making. Contents of the report will include:

1. Description of the subject and scope of the investigation
2. Description of each phase of the investigation, including all efforts
3. A chronology of the facts developed via the investigation
4. A description of remedial measures undertaken
5. A description of proposed corrective/preventative actions

VSD's will be drafted pursuant to Section 127.12(c)(2) of the ITAR, as a baseline, which include:

(i) A precise description of the nature and extent of the violation (e.g., an unauthorized shipment, doing business with a party denied U.S. export privileges, etc.);
(ii) The exact circumstances surrounding the violation (a thorough explanation of why, when, where, and how the violation occurred);
(iii) The complete identities and addresses of all persons known or suspected to be involved in the activities giving rise to the violation (including mailing, shipping, and e-mail addresses; telephone and fax/facsimile numbers; and any other known identifying information);
(iv) Department of State license numbers, exemption citation, or description of any other authorization, if applicable;
(v) U.S. Munitions List category and subcategory, product description, quantity, and characteristics or technological capability of the hardware, technical data or defense service involved;
(vi) A description of corrective actions already undertaken that clearly identifies the new compliance initiatives implemented to address the causes of the violations set forth in the voluntary disclosure and any internal disciplinary action taken; and how these corrective actions are designed to deter those particular violations from occurring again;
(vii) The name and address of the person making the disclosure and a point of contact, if different, should further information be needed.

SECTION 2 - Key Issues in University Research

2.1 Deemed Exports

While exports are commonly associated with the shipment of a tangible item across the U.S. border, export controls have a much broader application. One of the most difficult issues with respect to export controls is the fact that an export is defined to include the transfer of controlled *information or services* to foreign nationals even when the transfer takes place within the territory of the United States.

Under the EAR and ITAR, a transfer of controlled technology, source code, technical data, or defense services to a foreign national is deemed to be an export to the national's country even if the transfer takes place in the United States.

Stated differently, if you need an export license to export a controlled item/technology/software to the national's country, you need an export license to release the technical data about the item (ITAR) or to transfer the technology required for development, production, or use of the item to the person or entity in the United States. Technical assistance related to a development of a controlled item is also subject to this rule. The "*Deemed Exports Rule"* has been in place for decades and is most applicable in a university environment.

While a university may be involved in the shipment abroad of equipment or machinery to participate in a conference, a joint project, or equipment loan programs, most often faculty and students are engaged in teaching and research. Whenever teaching or research is related to controlled equipment or technology, the involvement of foreign students or researchers may trigger export control compliance issues.

The export may occur in several ways through:

1. A demonstration
2. Oral briefing
3. Telephone call or message
4. Laboratory or plant visit
5. Presenting at conferences and meetings
6. Faxes or letters
7. Hand-carried documents, hardware, or drawings
8. Design reviews
9. The exchange of electronic communication
10. Posting non-public data on the Internet or the Intranet
11. Carrying a laptop with controlled technical information or software to an overseas destination
12. Collaborating with other universities/research centers through research efforts

Keep in mind that if you are working with EAR99 technology, you may be required to obtain export licenses for foreign nationals/institutions that are on any of the "restricted parties lists" or when you are transferring the technology to embargo destinations.

2.2 U.S. and Foreign Persons

The regulations define a foreign person as anyone who is not a U.S. person. The BIS looks at the person's most recent citizenship and permanent residence. The DDTC looks at the person's country of origin (i.e., country of birth) and all current citizenships.

For purposes of defense and dual-use exports, a *U.S. person* is defined as a U.S. entity or a U.S. citizen, a person lawfully admitted for permanent residence in the United States (i.e., a green card holder), or a person who is a protected individual under the Immigration and Naturalization Act (8 U.S.C. § 1324b(a)(3) (i.e., certain classes of asylees).

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 (such as classified research).

Note that the definitions for a U.S. and a foreign person may differ for purposes of the OFAC sanctions. Contact the ECPOC for clarification or review the applicable OFAC sanction.

2.3 Public Domain or Publicly Available

- The EAR excludes publicly available technology if it is already published or will be published. Information is published when it becomes generally accessible to the interested public in any form, including:
    - Publication in periodicals, books, print, etc., available for general distribution free or at cost;
    - Readily available at libraries open to the public or university libraries;
    - Patents and open patent applications available at any patent office; or
    - Release at an open conference, meeting, seminar, trade show, or other gathering open to the public.
- The ITAR does not regulate information in the "public domain" nor is such information subject to licensing requirements. The ITAR has a very narrow scope of what is included within "public domain":

(a) *Public domain* means information which is published and which is generally accessible or available to the public:
(1) Through sales at newsstands and bookstores;
(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
(3) Through second class mailing privileges granted by the U.S. Government;
(4) At libraries open to the public or from which the public can obtain documents;
(5) Through patents available at any patent office;
(6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;
(7) Through public release (*i.e.*, unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also § 125.4(b)(13) of this subchapter);
(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the

scientific community. Fundamental research is defined to mean 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 the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. 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 or 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.

2.4 Marketing Information

- The ITAR (120.10(5)) states that technical data "does not include basic marketing information on function or purpose or general system descriptions of defense articles."
- The EAR (734.7) would include marketing information as qualifying for public release as being generally accessible and distributed to the interested public.

2.5 Educational Information

Both the ITAR and the EAR address the issue of general educational information that is typically taught in schools and universities. Such information, even if it relates to items included on the USML or the CCL, does not fall under the application of export controls.

- The EAR (734.9) states that educational information is not subject to the EAR if it is "released by instruction in a catalog course and associated teaching lab of academic institutions" (with the exception of certain encryption software and object code).
- The ITAR (120.10(5)) states that technical data "does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain…."

2.6 Patent Information

- The EAR (734.10) excludes "information contained in a patent application."
- The ITAR (120.11(5)) excludes "patents available at any patent office."

2.7 Fundamental Research

While some of FSU's projects involve applied research and may result in defense articles or technical data, FSU generally only undertakes projects that have the potential to make some contribution to the advancement of fundamental knowledge, primarily through publishable results**. FSU operates under the presumption that its research activities constitute "Fundamental Research" (as defined below) and that the results of such research may be generally published freely or shared within the academic community, except to the extent that (i) FSU explicitly agrees to publication or access restrictions requested in advance by the research sponsor; or (ii) some aspect of a particular research project is otherwise inconsistent with Fundamental Research.**

The EAR (734.8) describes Fundamental Research as follows:

(a) *Fundamental research.* "Technology" or "software" that arises during, or results from, fundamental research and is intended to be published is not subject to the EAR.

NOTE 1 TO PARAGRAPH (a): This paragraph does not apply to "technology" or "software" subject to the EAR that is released to conduct fundamental research. (See §734.7(a)(5)(ii) for information released to researchers that is "published.")

NOTE 2 TO PARAGRAPH (a): There are instances in the conduct of research where a researcher, institution or company may decide to restrict or protect the release or publication of "technology" or "software" contained in research results. Once a decision is made to maintain such "technology" or "software" as restricted or proprietary, the "technology" or "software," if within the scope of §734.3(a), becomes subject to the EAR.

(b) *Prepublication review.* "Technology" or "software" that arises during, or results, from fundamental research is intended to be published to the extent that the researchers are free to publish the "technology" or "software" contained in the research without restriction. "Technology" or "software" that arises during or results from fundamental research subject to prepublication review is still intended to be published when:

(1) Prepublication review is conducted solely to ensure that publication would not compromise patent rights, so long as the review causes no more than a temporary delay in publication of the research results;

(2) Prepublication review is conducted by a sponsor of research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers; or

(3) With respect to research conducted by scientists or engineers working for a Federal agency or a Federally Funded Research and Development Center (FFRDC), the review is conducted within any appropriate system devised by the agency or the FFRDC to control the release of information by such scientists and engineers.

NOTE 1 TO PARAGRAPH (b): Although "technology" or "software" arising during or resulting from fundamental research is not considered intended to be published if researchers accept restrictions on its publication, such "technology" or "software" will nonetheless qualify as "technology" or "software" arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

NOTE 2 TO PARAGRAPH (b): Research that is voluntarily subjected to U.S. government prepublication review is considered "intended to be published" when the research is released consistent with the prepublication review and any resulting controls.

NOTE 3 TO PARAGRAPH (b): "Technology" or "software" resulting from U.S. government funded research that is subject to government-imposed access and dissemination or other specific national security controls qualifies as "technology" or "software" resulting from fundamental research, provided that all government-imposed national security controls have been satisfied and the researchers are free to publish the "technology" or "software" contained in the research without restriction. Examples of specific national security controls include requirements for prepublication review by the Government, with right to withhold permission for publication; restrictions on prepublication dissemination of information to non-U.S. citizens or other categories of persons; or restrictions on participation of non-U.S. citizens or other categories of persons in the research. A general reference to one or more export control laws or regulations or a general reminder that the Government retains the right to classify is not a specific national security control.

(c) *Fundamental research definition. Fundamental research* means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.

The ITAR, Section 120.11, provides an exclusion from export control restrictions for information and technology already in the public domain, including technology resulting from "Fundamental Research" at universities and other institutions of higher learning. Section 120.11 of the ITAR describes public domain and fundamental research:

(a) Public domain means information which is published and which is generally accessible or available to the public:

(1) Through sales at newsstands and bookstores;

(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;

(3) Through second class mailing privileges granted by the U.S. Government;

(4) At libraries open to the public or from which the public can obtain documents;

(5) Through patents available at any patent office;

(6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;

(7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also §125.4(b)(13) of this subchapter);

(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean 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 the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. 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 or 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.

Both the ITAR and the EAR provide that information published and generally accessible to the public through fundamental research is not subject to export controls. However, there are certain restrictions. See 2.8 Fundamental Research Qualifiers below.

2.8 Fundamental Research Qualifiers

- Information results must be produced as part of basic and applied research in science and engineering and must be broadly shared within the scientific community (i.e., no restrictions on publication / dissemination of the research results);
- Information generated from the research is separate and distinguishable from the conduct that occurs in performance of the research;
- Even when the results of research are not subject to export controls, government approval may be required if the performance of the research requires foreign national access to export controlled technology. This may take the form of:
    - Proprietary/restricted information released to a foreign national;
    - Operation or use of export-controlled equipment in a manner that exceeds the deemed export threshold;
    - Mere access to a defense article.
- Research will not qualify as fundamental if the university (or the primary investigator) has accepted publication or other dissemination restrictions:
    - ITAR specifically identifies restrictions for proprietary reasons, or specific U.S. Government access and dissemination controls.
    - EAR specifies that fundamental research is 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. University-based research is not considered fundamental research if the university or its researchers accept restrictions (other than review to ensure no release of sponsor-provided proprietary or patent information) on publication of scientific and technical information resulting from the project.
    - National security controls include:
        - Restriction on pre-publication dissemination of information to non-U.S. citizens or other categories of persons;
        - Restrictions on participation of non-U.S. citizens or other categories of persons in the research. Pre-publication review and approval by the Government, with right to withhold permission for publication;

2.9 Proprietary or Restricted Information Provided by Research Sponsors (Updated 08/08/17)

The EAR and the ITAR provide that information received from government or corporate sponsors (i.e., "input" information) remains subject to the export control regulations when it is identified as proprietary or otherwise subject to access or publication restrictions. Information received from DoD that is designated as "Controlled Unclassified Information", "For Official Use Only", "Sensitive But Unclassified", or otherwise restricted, constitutes export controlled information and may not be released to foreign nationals, except as authorized under the ITAR or the EAR. Similarly, proprietary technical data and software applications received from corporate research sponsors or partners also would be subject to export controls.

The receipt of such controlled information, however, would not necessarily eliminate the availability of the Fundamental Research exemptions for the University's research results (i.e., "output" information). Where the university is able to conduct the research and publish the research results without disclosing the restricted input data to unauthorized persons, the research activities and results generally remain exempt from export controls under the Fundamental Research exemptions. In contrast, where it is not

possible to publish research results without disclosing restricted input data or software, such research results would be subject to applicable export controls.

2.10 Exports of Controlled Hardware, Software, and Related Technical Data

The Fundamental Research exemptions under the ITAR and EAR apply only to the information and technology developed through the research (i.e., "output" information). Hardware and software items produced in the course of research still may be subject to export controls when physically exported from the United States. Certain technical data relating to the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of such controlled applications also may be subject to export controls. (At the same time, "basic marketing information" or "general system descriptions" relating to the function or purpose of defense articles are exempt from controls pursuant to the Section 120.10 of the ITAR, unless specific contractual provisions state otherwise.)

In this regard, certain technologies may initially be researched for academic or commercial applications and regularly draw upon pre-contractual, FSU-developed technologies and software tools. These underlying technologies and software tools have broad research-related and commercial applications, and FSU regularly publishes its research findings in these areas. Where such underlying technologies and software tools are used or incorporated into a particular military application that is deemed to be ITAR-controlled, such usage should not subject those underlying technologies and software tools to the same ITAR controls. Thus, while FSU recognizes that it would need to restrict access to a specific military application in some cases (including the application itself and any application-specific source code and related technology), it would continue to treat its research relating to the underlying technology and software tools as Fundamental Research where appropriate.

FSU will, where appropriate, restrict access to specific military applications. Presentations, publications, facility tours, and other types of disclosures do not include or otherwise result in the release of ITAR-controlled technical data.

2.11 Defense Services

Finally, the Fundamental Research exemptions generally apply only to basic and applied research conducted in the United States. Pursuant to the ITAR's restrictions on "defense services," research involving the provision of military or defense-related technical assistance (i.e., "conduct") to foreign persons may require authorization under the ITAR, even where there are no contractual access or publication restrictions applicable to the research. Accordingly, FSU will apply for and obtain ITAR approvals for mere access to defense articles or technical data for foreign persons.

2.12 Full-Time University Employees

Under a specific exemption, the ITAR allows a university to disclose unclassified technical data in the U.S. to a foreign person who is the university's *bona fide* and full time regular employee. The EAR allows universities to transfer EAR controlled technology and source code to their bona fide and full time regular employees under the TSU – §740.13.

The EAR and ITAR exemptions are identical and available under the following circumstances:

- The employee's permanent abode throughout the period of employment is in the United States.
- The employee is not a national of a country to which exports are prohibited pursuant to ITAR §126.1 (See current list of countries at http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf).
- The university informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of the DDTC.
- The university documents the disclosure of technical data under the exemption providing:
    - A description of the technical data,
    - The name of the recipient/end-user,
    - The date of export,
    - The method of transmission (e.g., email, fax, FedEx), and
    - The ITAR/EAR reference:
- For ITAR: 22 CFR 125.4(b)(10), *Disclosures of unclassified technical data in the U.S. by U.S. institutions of higher learning to foreign persons who are their bona fide and full time regular employees*
- For EAR: 15 CFR 740.13(f), *Release of technology and source code in the U.S. by U.S. universities to their bona fide and full time regular employees.*

Note that the "full-time *bona fide* employee" requirement will preclude foreign students and postdoctoral researchers from qualifying for access to technical data under this exemption. Generally, a H1B work visa would be required.

This exemption only applies to the transfer of *technical data* and discussions related to the data. Discussions may occur between the foreign full-time employee and other university employees working on the project. Additionally, the outside company (sponsor of the research) would have to apply for a DSP-5 license to provide technical data directly to the foreign national employee, and if the outside party and the employee are to engage in discussions and interchange concerning the data, then the proper authorization may be a Technical Assistance Agreement (TAA).

Contact the ECPOC to help you determine if the exemption applies and document the exemption.

2.13 Graduate Thesis

Any graduate student that is working on ITAR controlled research to fulfill his or her thesis requirement must be a U.S. Person; otherwise, the University will be required to submit an export license for him/her to work on the controlled research. If the student includes technical data in the graduate thesis, the publication must be approved by either the Cognizant Government Agency or Office of the Security Review prior to the publication as required by the regulations. It is important to recognize that the publication approval might be delayed and ultimately, publication of certain data may be denied for national security reasons. Moreover, the thesis advisory committee and defense committee must only include U.S. Persons unless an export license has been secured prior to their participation.

2.14 Visa Applications

This process addresses theI-129 certification process for visa applicants who may have access to export controlled items.[1] It also addresses the process for using the bona fide employee license exemption for allowing foreign national access to ITAR/EAR items and/or data.

In 2010, the Department of Homeland Security, U.S. Citizenship and Immigration Services issued new requirements in connection with obtaining certain visas for faculty and staff. Specifically, the I-129 Form (used in connection with H-1B visas for temporary workers, O-1 visas for persons of extraordinary ability, and TN (Trade NAFTA) visas) includes a certification concerning export controls. As part of its I-129, H1 Visa Application process, the U.S. Immigration and Citizenship Service (USCIS) requires a certification as to whether the Beneficiary will require an export license to access export controlled technology or technical data during the course of his/her professional position. If a license is required, the Certification also requires the Petitioner to state that it will prevent access or disclosure through a control plan until a license is approved by the Department of Commerce or State. Note that in certain cases, the U.S. Government might not issue a license for particular sensitive control reasons.[2]

As a result, in advance of the H1 visa petition being submitted to FSU's Center for Global Engagement, it is critical to evaluate whether access will require an export license, the likelihood of obtaining a license, or the need for an interim or permanent Technology Control Plan. FSU must assess precisely what controlled technology or technical data it has or plans to have which could be accessed by an H1 employee. Toward this objective, the pertinent faculty members and administrators shall complete FSU's Form I-129 Export Control Certification Questionnaire and submit the form to the Center for Global Engagement during the recruitment process.

2.15 International Collaboration and Exchange Agreements

This subsection addresses the process for managing the export control requirements associated with international collaborations with potential international research partners. Several export control requirements are applicable:

1. When drafting or planning to sign a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) with a potential non-U.S. research partner that does not directly fall under the auspices of Sponsored Research Administration or the FSU Research Foundation, the faculty member planning to enter into such an agreement must alert the ECPOC so that any export control implications to the proposed agreement can be evaluated in advance.
2. Prior to signing such an agreement, FSU shall screen such entity and signatories against the U.S. Government's watch lists to ensure that potential partners are not listed.
3. MOUs or MOAs may contemplate the exchange of export controlled items or data that drive the collaborative research. Because the export of such items or their receipt into FSU's laboratories potentially has export control implications, these implications must be identified at the earliest opportunity so that the parties can plan accordingly. In certain cases, where the research is predicated on the receipt of (or access to) an export controlled item that requires prior government approval through a license or authorization, it is important that the parties take this contingency into account either in the MOU/MOA process or in a subsequent writing. FSU cannot bind itself to a contractual obligation without acknowledging the need to fulfill a regulatory condition without which the program cannot proceed as intended.

4. Subsequent amendments to the MOU/MOA must proceed according to the same evaluation process, to the extent they subsequently alter the terms of the initial MOU/MOA or where the parties/signatories change over time.
5. When the MOU/MOA contemplates concurrent or subsequent Non-Disclosure Agreements (NDAs) and/or the receipt of export controlled items or data, contact the ECPOC to determine the precise export control language that shall be inserted into the NDA. The purpose of this language will be to alert FSU in advance of a party's intention to provide export controlled items, so that FSU can determine the correct handling and disposition of such items consistent with control requirements or, where appropriate, decline acceptance of these items.

2.16 DOD form DD2345, Militarily Critical Technical Data Agreement (Updated 08/17/17)

The United States/Canada Joint Certification Program (JCP) was established in 1985 to allow U.S. and Canadian contractors to apply for access to U.S. Department of Defense (DOD) and Canadian Department of National Defence (DND) unclassified export controlled technical data/critical technology on an equally favorable basis in accordance with U.S. and Canadian Regulations. More information about the U.S./Canada Joint Certification Program is available here.

The joint certification is effected through a *Militarily Critical Technical Data Agreement* (DD2345) between FSU and the Joint Certification Office. The DD2345 is required for U.S. contractors or subcontractors who wish to obtain access to unclassified technical data disclosing militarily critical technology with military or space application that is under the control of, or in the possession of, the DOD.

This certification can be used to facilitate visits to U.S. military installations that involve access to unclassified technical data. Activities intended to be covered under the DD2345 include:

- Procurement activities such as pre-solicitation conferences;
- Discussions related to unclassified solicitations;
- Collection of procurement unclassified documents (RFQ's, RFP's, bid sets, etc.);
- Performance of an unclassified contract;
- Scientific research, in a professional capacity, in support of unclassified U.S. defense initiative;
- Attendance at restricted meetings, conferences, symposia, or program briefings where technical data governed by DOD Directive 5230.25 will be presented.

The government currently allows only one certification per university. FSU's DD2345 is managed by the ECPOC. If an FSU employee or student is asked for a DD2345 as a condition of attending a conference or receiving materials from the U.S. government, contact the ECPOC and provide the following information:

- Meeting attendee name
- Country of birth and current citizenship
- Purpose, location, and dates of the meeting
- Information/technical data to be provided to attendee
- Information/technical data to be brought back to FSU by attendee, or sent directly to ORCP.

The ECPOC will review the circumstances of the request, and if appropriate, implement a Technology Control Plan (TCP) for handling the controlled information. The TCP is a vehicle used by FSU to manage access to EAR- and ITAR-controlled objects, services, and technical data. The TCP must be kept current while the controlled objects, research, or data is at FSU. The TCP should be in place before the meeting if at all possible. The ECPOC will debrief the attendee upon his/her return to FSU, and update the TCP as appropriate. In some circumstances, the technical data will need to be sent directly to the ECPOC. More information on TCPs is located in Section 5.3.

SECTION 3 - FSU Management Structure and Policy

3.1 Institutional Commitment

As a leading academic institution on the forefront of technological development and academic research, Florida State University will strive to educate and conduct research in harmony with the export control laws, regulations, and sanctions of the United States. A preponderance of activities taking place at FSU are educational in nature, consisting of basic and applied research, the fruits of which are intended for learning and open distribution among scientific and technical communities. While the University recognizes that education is based primarily on the free and open exchange of information and ideas, it occasionally consciously chooses to accept research and conduct activities subject to proprietary or national security restriction that nullify free and open exchange and subject such efforts to limitations on access and distribution. To fulfill its commitment, the University has established the Office of Research Compliance Programs to collaborate with various academic departments and research units engaging in activities subject to export controls to:

- Support FSU's commitment to comply with U.S. export control policies, laws, regulations, and sanctions;
- Provide direction and solutions to researchers, faculty, staff, and employees in complying with export controls;
- Prevent inadvertent transfers of export controlled technologies;
- Educate, train, and foster compliance.

Most research and activities conducted on-campus are excluded from U.S. export control laws, including the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) sanction regulations. However, certain research involving specified technologies controlled under the EAR or the ITAR, or transactions and exchanges with designated countries or sanctioned entities may require that the University to obtain an export license or other government approval prior to providing controlled technologies to certain foreign national employees, professors, students, researchers, or other foreign national collaborators. However, information generated during the course of "Fundamental Research", as defined under such laws, is exempt from export licensing requirements.

The University will fully comply with U.S. export control laws while ensuring that, to the extent possible, university instruction and research is conducted openly and without restriction on participation or publication. To this end, the University will ensure that, unless unavoidable, information generated during the performance of any university research, including sponsored contract activities, qualifies for the Fundamental Research provisions of applicable export control laws. The civil and criminal penalties associated with violating export control regulations can be severe, ranging from administrative sanctions, including loss of research funding, to monetary penalties to imprisonment for individuals.

The University is committed to educating its employees, professors, students, researchers, or other collaborators on U.S. export control laws and regulations and their particular application within a university research setting. As part of the University's ongoing commitment to export control compliance and education, the University has established a website at: http://www.research.fsu.edu/research-compliance/export-controls/ that contains the university export control policy, forms, and training and reference materials.

3.2 Export Control Policy

FSU's Policy on Export Controls is published at: http://www.research.fsu.edu/research-compliance/export-controls/.

3.3 Empowered Officials

If a project is export-controlled and a license is needed for any purpose, only an Empowered Official may register with the Directorate of Defense Trade Controls (DDTC) pursuant to 22 CFR Part 122 and apply for the export license. In the event registration is required, only individuals in the following university positions may be designated as Empowered Officials:

- Vice President for Research
- Research Legal Counsel
- Director of Research Compliance Programs

In this capacity, designated Empowered Officials:

(1) Are directly employed by FSU in a position having authority for policy or management; and
(2) Are legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of FSU with the U.S. State Department; and
(3) Understand the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations; and
(4) Have the independent authority to:
(i) Enquire into any aspect of a proposed export or temporary import by FSU;
(ii) Verify the legality of the transaction and the accuracy of the information to be submitted; and
(iii) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

SECTION 4 - University Roles and Responsibilities for Export Control Compliance

4.1 Office of the Vice President for Research

The Vice President for Research (VPR) is the university official with final responsibility for compliance with export- and sanction-related regulations.

4.2 Office of Research Compliance Programs

The functional administrative unit at Florida State University charged with the responsibility for oversight of compliance and recordkeeping of all applicable exports and regulated transactions with sanctioned individuals, entities, and countries is the Office of Research Compliance Programs (ORCP), a unit under the Vice President for Research. FSU's Export Controls Point of Contact (ECPOC) is Diana Key, Director, Research Compliance Programs at dkey@fsu.edu or (850) 644-8648.

The ECPOC is the principal point of contact for all export control and related activities throughout the university. The ECPOC is the designated Empowered Official charged to oversee, administer, and coordinate all export compliance functions in concert with other departments and units as necessary, including:

- Manage the support functions to other University departments and units, including:
  - Performing agreement reviews and analysis;
  - Conducting export assessments of international shipping, transfers, and travel;
  - Prepare, review, approve, and submit license applications for international exports and deemed-exports, and other requests for government agency export approval;
  - Determine the application of licensing exceptions or licensing requirements and exception/exemption certificates as applicable; and
  - Research, prepare, approve, and submit advisory opinion requests or other government guidance requests.
- Provide subject matter expertise on University policy and procedures related to export controls.
- Develop and deliver export control education and awareness to the broad University community.
- Provide strategic consultation and guidance to faculty, staff, and administration on decisions that have import/export regulatory impact.
- Identify project-specific sensitive material concerns. Collaborate with Principal Investigators and technical research staff to identify sensitive information and equipment. Using information from a variety of internal and external sources, determine commodity jurisdiction and self-classify equipment and technologies pursuant to ECCN or USML classifications and implement and maintain automated self-classification decision tools (Visual Compliance).
- Make immigration related export certifications and conduct technology alert investigations, as required by the U.S. Consulate. Review H-1B and other foreign national beneficiary information as it relates to deemed export and licensing needs. Work with other campus units as needed to acquire and review associated agreements and technology/data or software associated with foreign national activity at the University. Review and approve deemed export control attestations on behalf of the University. Manage federal background investigations, personnel security clearances, and visit authorizations for employees, consultants, and cleared visitors, as needed.
- Liaison with federal regulatory and investigatory agencies (e.g., Commerce, State, Treasury, Energy, Defense, DSS, FBI) regarding export control matters to counteract illegal foreign intelligence gathering methods, identifying breaches/spillages, and providing intelligence for ongoing investigations. Assist federal agencies in the identification and neutralization of foreign interdiction of sensitive U.S. technology, articles, and data identified as export controlled and act as liaison and coordinator for export-related and travel matters between the various research and regulatory offices within FSU.

4.3 Research Legal Counsel

The Research Legal Counsel serves as the legal advisor to the ECPOC on issues associated with export control compliance.

4.4 Sponsored Research Administration and the FSU Research Foundation (Updated 8/08/17)

In close coordination with the ECPOC, Sponsored Research Administration (SRA) and the FSU Research Foundation (FSURF) ensure that all sponsored activities are managed in accordance with the FSU'S Policy on Export Controls and this Plan. SRA/FSURF personnel are trained to assess potential export control issues associated with FSU programs and route all assessments to the ECPOC for final disposition.

SRA/FSURF—as reviewers of solicitations, proposals, and awards—performs the export control *initial review* by looking for the following red flags indicating possible export control issues:

- References to U.S. export regulations.
- Restrictions on publication or dissemination of the research results.
- Pre-publication approval from sponsor.
- Indication from the sponsor that export control information will be provided for the research (e.g., requirement for a DD 2345, Militarily Critical Technical Data Agreement).
- Proprietary or trade secret claims on project results.
- Restriction of access or participation to U.S. citizens only.
- Involvement of foreign sponsors or collaborators.
- Travel, shipping, or work performed outside the U.S.
- Information/data protection requirements.
- Military applications of the project results.
- Research conducted by high risk areas such as space, physics, engineering, computing, chemistry, and microbiology.
- Research involves spacecraft systems and equipment, unmanned air vehicles, nuclear design, toxins, computers, electronics, encrypted software, lasers and sensors, chemicals, and microorganisms.
- Reference to the words "sensitive but unclassified" or "controlled unclassified information" in the proposal or award.
- Funding from Defense or Intelligence Agencies, the Department of Energy, NASA, or other U.S. government agencies.

If the *initial review* flags a possible export controls issue, the project will be referred to the ECPOC for final review. The ECPOC is responsible for negotiating acceptable terms and conditions related to export control compliance, in consultation with the Principal Investigator. Upon completing the *final review*, the ECPOC will advise SRA/FSURF and the PI concerning any export controls that apply to the project, the restrictions on access by foreign persons, and any other relevant requirements pursuant to ITAR, EAR, OFAC, and other regulations.

4.5 Vice Presidents, Deans, Directors, and Chairs

Deans, Directors, and Chairs (and any Vice President that act as Dean for a center/institute) share the responsibility of overseeing export compliance in their respective units, and working with the ECPOC to implement effective processes and controls to ensure export control compliance.

4.6 Principal Investigators/Researchers

Principal Investigators (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 in class with fellow researchers or collaborators. PIs must ensure that they do not disclose controlled information or transfer-controlled articles or services to a foreign national without prior authorization as required.

To meet his or her obligations, each PI must:

- Understand his or her obligations under export controls, and participate in regular trainings to help him or her identify export control issues.
- Provide the ECPOC with all required documentation and guidelines provided by the contracting agency to ensure compliance with export controls.
- Assist the ECPOC to classify the technology involved in the research or other university activity.
- Identify foreign nationals that may be involved and, if the research is subject to export restrictions, initiate the process of clearing foreign national participation well in advance to ensure that a license is obtained in a timely manner, or implement proper measures to isolate foreign nationals from participation.
- If undertaking an export-controlled project, brief the students and other researchers involved in the project of their obligations under export controls or ask the ECPOC to do so.
- Cooperate with the ECPOC in developing the Technology Control Plan when needed.
- Ensure that all physical exports comply with the foreign trade regulations, import requirements in the destination country, and that all shipping paperwork is accurate and records of all shipments are kept on file for at least five years from the date of export.

4.7 Other Support Personnel

Other personnel, including Administrative and Professional (“A&P”) staff, students, post docs, and other support staff, provide critical support to export controls by identifying potentially problematic export control issues and forwarding those issues for assessment, including deemed exports; international shipping; import of goods; and reporting of suspicious incidents.

4.8 Office of Commercialization

In coordination with the ECPOC, the Office of Commercialization (OC) ensures that all patent applications are secured until such time as they are filed and become “publicly available.” Fundamental research generated technology and information contained in the patent application is not public domain until the patent is processed, typically 18 months after submission. Information about the invention that is not publicly disseminated via the patent application, journal articles, or other public venues is not public domain. Information left out of the patent, patent application and other publicly available documents such as know-how is not public domain. The OC coordinates with the ECPOC to implement the necessary security protocols for all patent applications subject to a secrecy order.

4.9 Office of Inspector General Services

The Office of Inspector General Services (OIGS) provides feedback to the ECPOC on compliance with export controls requirements during routine scheduled departmental and college audits. Export information necessary for these audits is shared with OIGS so that a thorough examination can be conducted. On a case-by-case basis, OIGS conducts targeted research and data collection in close coordination with the ECPOC for official investigations.

4.10 Environmental Health and Safety

The Environment Health and Safety (ESH) office provides assistance with shipping, receiving, storing, and using hazardous materials that are export controlled. More information about EHS can be found at https://www.safety.fsu.edu/.

4.11 Finance and Administration

[Under development.]

4.12 Reserved

4.13 Reserved

4.14 Center for Global Engagement

The Center for Global Engagement works closely with international students, providing support related to their F or J visa status. It also services related to H-1B visa. More information about the Center can be found at https://cge.fsu.edu/.

4.15 Information Technology Services

Florida State University's information security and privacy policies and procedures effectively addresses the need to protect confidential and sensitive information that is maintained in the various spheres of University activities, including export controlled technical data. The research setting poses particular information security risks and challenges, including regulatory and contractual constraints that require additional policy provisions and protective measures. To protect research data appropriately and effectively, FSU's researchers, research oversight bodies, and information technology staff must understand and carry out their responsibilities related to data security.

The Information Security and Privacy Office (ISPO), which operates as a division of Information Technology Services and reports to the Chief Information Officer and Provost, is dedicated to its mission to ensure the confidentiality, integrity and availability of FSU data and to protect the privacy of the information entrusted to our university. Its team does this by focusing on the following key areas:

- Policy
- Training and Outreach
- Risk Management
- Operations and Incident Management

- Survivability

ISPO's website serves as a central resource for guidance on a wide range of privacy issues affecting the campus community. The site includes an overview of the services they provide to campus and important university information security and privacy policies, as well as information on how to protect your data and the university from cyber threats.

4.16 Reserved

SECTION 5 - Processes and Procedures

5.1 Information Technology

This Section addresses the process for protecting export controlled proprietary technical data and when these protections are required, including travel with clean laptops.

While certain standard IT protocols will be adequate to address EAR and ITAR requirements, others (particularly with regard to unauthorized Foreign National access) will have to differentiate between ITAR and EAR controls. Typically, IT requirements will have to address, among other things, the following areas: laptop security, network security, back-up and storage applications, file access approval (including download and print permissions), and email protocols. ITAR and EAR controlled technical data must be securely limited to approved access only.

For assistance with export control IT procedures, please contact Mike Boll, Research Data Security Specialist in ITS/ISPO at mboll@fsu.edu.

5.2 Physical Security

This subsection addresses the process for physically securing ITAR and other controlled items where applicable in FSU's research facilities.

Within facilities containing ITAR and EAR-controlled items (equipment, materials, software, and technical data), FSU is required to maintain safeguards that prevent unauthorized physical and/or visual access to such items, depending on the applicable deemed export situation.

Depending on the particular control requirement, access restrictions may apply to FSU personnel, as well as to visitors (vendors, research collaborators, service technicians, etc.). Where foreign national personnel are authorized by license to access controlled items, such personnel and their Principle Investigators or supervisors/managers must be fully aware of the limits of such access as provided for in the license and/or its provisos and in the particular Technology Control Plan.

The ECPOC will assist departments with determining whether or not special access controls are required for a given space, and if necessary, prepare an appropriate Technology Control Plan.

5.3 Technology Control Plans

Development

If the ECPOC determines that a project is export controlled, the ECPOC will take the lead and work closely with the PI to develop and implement a technology control plan (TCP) to secure the controlled technology from access by unlicensed non-U.S. citizens. Sometimes a TCP may be necessary to secure a particular laboratory or research facility.

The TCP will generally include:

- A commitment to export controls compliance
- Purpose and scope of the plan
- Identification of the relevant export control categories and controlled technologies
- Overview of applicable regulations
- Application of export regulations to the project
- Identification of the project's sponsors
- Non-disclosure statement from each research project participant
- List of export licenses and license exceptions applied to the project
- Appropriate physical and informational security measures
- Personnel screening measures
- Research lab visitor's policy
- Record keeping policy
- Export compliance training and training logs
- Appropriate security measures for and following project termination
- Statement on Reporting violations
- Annual audit record

Security Measures

The TCP will include physical and informational security measures appropriate to the export control categories involved in the project. Examples of security measures include, but are not limited to:

- Laboratory Compartmentalization: Project operation may be limited to secured laboratory areas physically shielded from access or observation by unauthorized individuals. These areas must remain locked at all times.
- Time Blocking: Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access.
- Marking: Export controlled information must be clearly identified and marked as export controlled (either "ITAR controlled" or "Controlled under EAR").
- Personnel Identification: Individuals participating in the project will be listed in the TCP and only authorized personnel will have access to controlled laboratories.
- Locked Storage: Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key-controlled access. Soft and hard copy data, lab notebooks, reports, and other research materials should be stored in locked cabinets.
- Electronic Security: Project computers, networks, and electronic transmissions should be secured and monitored through User Ids, password controls, Secure Sockets Layer encryption or other federally approved encryption technology. Database access should be managed via a Virtual Private Network.
- Confidential Communications: Discussions about the project must be limited to the identified and authorized project participants, and only in areas where unauthorized individuals are not

present. Discussions with third party sub-contractors must occur only under signed agreements which fully respect the non-U.S. citizen limitations for such disclosures.

Training and Certification

Before any individual may observe or access the controlled technology, he or she must be briefed on the procedures authorized under the TCP, certify his or her agreement to comply with all security measures outlined in the TCP, and have his or her certification authorized by the ECPOC.

Note: In cases where a U.S. Government agency wishes to review a TCP as part of a licensing procedure or as part of an audit process, the PI and/or administrator in charge of implementing the TCP shall notify ECPOC of such a request so that appropriate oversight is in place.

5.4 Procurement

This subsection addresses the identification of export-controlled items and materials in the procurement process, and communicating any control status of the item to the buyer or user on campus.

It is important that in those instances where FSU purchases a controlled item or material for research or educational purposes, said item must be identified as such, and the controlled status communicated to the user on campus (e.g., principal investigator, lab/program administrator, etc.) and ECPOC. Therefore, the following term/condition shall apply to each purchase order issued by FSU:

> Export Control. The parties shall comply with all applicable U.S. export control laws and regulations, including but not limited to the International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120 through 130, the Export Administration Regulations (EAR), 15 CFR Parts 730 through 799 and/or other restrictions imposed by the Treasury Department's Office of Foreign Asset Controls (OFAC), in the performance of this PO/PO. The parties agree that no technology, related data or information will be exchanged or disseminated under this PO nor any collaborations conducted pursuant to this PO, which are export controlled pursuant to the export control laws of the United States, including the EAR and the ITAR and any other applicable regulations. The Parties agree that the Supplier will not provide FSU with any ITAR or EAR restricted technology and/or related data, and that any ITAR or EAR restricted technologies and/or data produced in furtherance of this PO will be in the exclusive possession of the Supplier and at no time will any export controlled technologies, related data, or information be intentionally or inadvertently transferred to FSU, its facilities, labs, staff, researchers, employees, officers, agents, servants or students in the performance of this PO. If the Supplier wishes to disclose export controlled technology or technical data to FSU, the Supplier will, prior to disclosing any information, technical data or source code that is subject to export controls under federal law, notify FSU in writing that the material is export controlled and shall identify the controls that apply. FSU shall have the right to decline or limit (a) the receipt of such information, and (b) any task requiring receipt of such information. In the event the Supplier sends any such technical data or product that is subject to export control, without notice of the applicability of such export control, FSU has the right to immediately terminate this PO. The Supplier understands and agrees that to the extent the Supplier's personnel have access to work or materials subject to U.S. export controls while on FSU property, such personnel will meet all federal export control regulatory requirements or have the appropriate U. S. government approval. (FSU Purchase

Order/Contract Standard Terms and Conditions. Retrieved on April 7, 2015 from http://procurement.fsu.edu/sites/default/files/media/doc/StandardTermsandConditions.pdf.)

If the supplier of scientific or technical equipment or technology does not know the export control status of an item (e.g. when the supplier is not the manufacturer) or refuses to provide export control information to the University, ECPOC may perform a self-determination based on the available information. If the jurisdiction of the item(s) is unknown, the University may request a commodity jurisdiction or advisory opinion, as appropriate. In cases where the ECCN/USML number is other than EAR99, ECPOC must be notified and a TCP established required.

In the event export-controlled items or data are accepted by FSU and once the supplier has identified a control status, this information shall be transmitted to the laboratory director or administrator and ECPOC. ECPOC shall likewise maintain a database of all such items so that access restrictions and outbound export of these items (ITAR or EAR) are appropriately flagged for potential licensing.

Export Control Notices

Should an export control notice be included with the shipped items, please forward it to the ECPOC by scanning it and sending it as an email attachment. If the notice states that an item is subject to the Arms Export Control Act, ITAR, or Department of Energy export control regulations (10 CFR 110 or 810), the recipient should immediately secure the subject item from access by foreign nationals and notify the ECPOC for assistance.

5.5 Licensed Software Programs

This subsection addresses the export control implications of licensing a software product that has been identified as “export controlled” by the software licensor or vendor.

Certain software products may be identified by the licensor or vendor as “export controlled.” In such cases and for purposes of understanding access implications for FSU, it is necessary to determine whether the control notification is a general notification for purposes of alerting the user against exporting to OFAC-restricted countries, or whether a more specific control is applicable as may be the case with cryptographic functionality or ITAR-governed software.

Where the software is flagged for general purposes, it is no different than any other item which FSU might, in turn, export; however, restrictions against exporting to sanctioned/embargoed countries apply under both OFAC and EAR regulations. Where, on the other hand, the item is more specifically controlled (e.g. due to cryptographic functionality or as an ITAR defense article), FSU may be required to implement a Technology Control Plan and evaluate the article for export licensing where outbound export is contemplated.

For assistance in making these determinations, please contact the ECPOC.

5.6 Biosafety

Risk management protocols also require that the transfer of biological materials by FSU to another institution strictly adhere to FSU’s protocols. In certain cases, such materials may also be export

controlled under the EAR and in rare cases under the ITAR. As such, the exporter shall work directly with Environmental Health and Safety to determine whether export control requirements are being met and what if any special arrangements (including export licensing, destination control statements, and end user agreements) shall be affected pursuant to such international transfers. EHS and the exporter will work with ECPOC to establish a TCP if one is required. For assistance in making these determinations, please contact the ECPOC or FSU Biological Safety Office (644-5374, 644-9117, or 644-6895).

5.7 Material Transfer Agreements and Non-Disclosure Agreements

This subsection addresses the export control requirements associated with Material Transfer Agreements.

Because the transfer of technology and/or materials pursuant to a Material Transfer Agreement (MTA) may trigger export control requirements, the Research Legal Counsel shall work directly with the ECPOC to proactively identify and resolve export control requirements associated with an MTA. Such requirements maybe triggered when the activity contemplates an international transfer, or is domestic within the U.S. but FSU has knowledge that the item will be re-exported by the receiving party. As applicable to the transaction at hand, the MTA shall take into account necessary export control provisions that include but are not limited to notification of export control status (ITAR or EAR), as well as general end use/user restrictions and applicable destination control statements.

Incoming Non-Disclosure Agreements (NDAs), where FSU is requested to sign another party's confidentiality agreement covering the receipt of proprietary items or data must likewise be reviewed and provisioned for export control purposes. As the potential modification of another party's agreement can take additional time, the Research Legal Counsel shall be alerted as soon as possible to a pending agreement so as to allow sufficient opportunity for timely evaluation.

For assistance with technology transfer agreements, please contact the ECPOC.

5.8 International Travel (Updated 08/10/17)

When you travel internationally as an employee, student, principal investigator, or fellow of Florida State University ("FSU"), you need to know your responsibilities under U.S. export control regulations. Traveling abroad and taking certain items, providing certain services, or meeting with certain people can present export control problems. This document provides guidance on how to avoid running afoul of U.S. export control regulations when traveling internationally.

Travel to most countries does not present an export control problem; however, travel to some countries may present a problem that is easily addressed, if we create and maintain records that show that the travel was exempt from the export control regulations. Even so, when an export control license is required for travel, it is crucial that we obtain it prior to the trip as violations of U.S. export control laws carry severe civil and criminal penalties for both FSU and the offending individual in violation of the regulations.

Sanctioned Countries/Restricted Parties

Certain foreign parties – including specific people, businesses, research institutions, universities, government and private organizations, and other types of legal persons – may be subject to federal U.S. prohibitions. Such prohibitions may include prohibitions on research collaborations and may require

specific licensing, even for educational exchange. These prohibitions are specified on several federally-maintained restrictive lists. It is important to review these lists and understand compliance responsibilities and limitations before collaborating, or sponsoring an employee or visiting scholar of a university listed therein.

FSU uses Visual Compliance™ to expedite screening of the restrictive party lists. Educational exchange, including travel to any entity on any of the restrictive lists, has specific license requirements, and exemptions typically do not apply. The government has a policy of denial for licensing many of the entities on the lists. Before you travel, contact the ECPOC for further guidance.

Purpose of the Trip

Presentations & Seminars: In general, travel outside of the U.S. to attend a conference (but not to present) does not require a license. However, if you present at a conference, the material must be limited to topics that are not related to export-controlled items or technologies, unless that information is already in the public domain. Open seminars are usually not problematic unless they take place in a sanctioned country or involve restricted parties. Exchanges of technical information including academic discussions could require a license.

Foreign Collaborations & Exchanges of Technical Information: Publicly available information or fundamental research can be shared with foreign colleagues as long as the recipients are not employees or representatives of the government of a sanctioned country, or restricted parties. This collaboration includes normal academic peer-review or publishing processes.

Research & Instruction Outside of the U.S.: Research and course instruction conducted outside of the U.S. may not qualify for the fundamental research exclusion. Export control regulations may apply until the work is published or is otherwise in the public domain. Before teaching a course or disclosing information outside of the U.S., it is important to ensure that the information is not subject to export control laws and regulations. For instance, when interacting with foreign persons, you cannot provide a "defense service" which includes providing technical "know-how" related to the design, development, production, manufacturer, assembly, operation, repair, testing, maintenance or modification of a defense article or dual-use technology.

Furnishing Financial Assistance: OFAC regulations prohibit providing material financial assistance or anything of value, including services, to any blocked or sanctioned country, individual, entity or organization, including a government agency of a sanctioned country. This can involve subcontracts, international suppliers, or payments to research participants. For example, a professional presentation, **whether or not it contains materials controlled under International Traffic in Arms Regulations ("ITAR") or Export Administration Regulations ("EAR")**, is a "service" and "something of value" provided to the recipient audience, under OFAC regulations.

Export of Equipment or Data

Any tangible items that you take to a foreign country are considered "exports" by the U.S. Government, even if you are planning to bring the items back upon your return.

Even the technical information located on your laptop's hard drive is considered to be an export of technology/technical data, once the laptop or notebook leaves the U.S. If you are traveling abroad with your laptop or any other electronic devices, these items along with the underlying technology, any data on your device, proprietary information, confidential records, and encryption software are all subject to U.S. export control regulations. Some foreign governments have regulations that permit the seizure of travelers' computers and the review of their contents. U.S. Customs officials are also authorized to review the contents of travelers' laptops without probable cause and can be held until your return.

You must comply with U.S. export regulations whenever you take such equipment and data outside of the U.S. Items that could have a "dual-use" (both commercial and military or proliferation applications), proprietary information, or items that are considered defense articles (even if used in an academic or research environment) are generally prohibited from export without specific federal licensing. Export control regulations will generally not restrain you from taking commercially available laptop computers and standard software to most countries. In most situations, licensing is not required to take items abroad under the Temporary Export Exception (TMP) as a "tool of trade." However, other research equipment, select agents and toxins may not qualify under this exception. To qualify for the "tool of trade" exception, the export must:

(1) Remain under the effective control of the exporter (or the exporter's employees) by retaining physical possession of the equipment at all times or securing the item in a secure environment;

(2) Consist only of reasonable equipment of the trade (equipment that people in your discipline would generally recognize as a "tool of trade");

(3) Not be to an embargoed country (Cuba, Iran, North Korea, Syria, or Sudan);

(4) Be carried with the exporter or shipped ahead within 30 days of exporter's travel;

(5) Be data that is within the public domain; and

(6) Be for less than one (1) year.

You should not take ANY of the following items abroad without first obtaining specific advice from the ECPOC:

(1) FSU-owned scientific equipment (other than a sanitized laptop computer, PDA, smart phone, or electronic storage device);

(2) Data or information received under an obligation of confidentiality including private information about research subjects;

(3) Data or analyses that result from a project for which there are contractual constraints on the dissemination of the research results;

(4) Devices, equipment or computer software received with restrictions on export to or on access by foreign nationals;

(5) Devices, systems, or software that was specifically designed or modified for military or space applications; or

(6) Classified information.

If U.S. Customs and Border Protection (CBP) officials suspect that a regulated item or defense article has been exported without a license, they may, for example, on your return examine files and software on your laptop computer as well as your baggage. For this reason, international travelers are encouraged to "sanitize" electronic devices by removing all non-essential data prior to leaving the United States. **Inspectors in other countries may detain and copy your hard drive.** Alternate safeguard methods include taking a sanitized laptop with only public domain files needed for the specific international trip or encrypting and then e-mailing to yourself any information you may need while overseas. Do not retrieve the e-mail until you have reached your destination, and remember you will need to remove it completely prior to returning to the U.S. or prior to crossing any international border.

FBI Tips:

Safety and Security for US Students Traveling Abroad

Safety and Security for the Business Professional Traveling Abroad

U.S. Department of State, Travel Alerts and Warnings, Cuba Travel

Best Practices

Tips from the University of Pennsylvania:

http://www.upenn.edu/computing/security/advisories/InfoSec_Data_Security_Travel_Tips.php

Travel Tips from California Polytechnic State University:

http://www.security.calpoly.edu/content/practices/travel_tips

Presentation from Northwestern University:

http://www.it.northwestern.edu/bin/docs/TT_Travel.pdf

Northwestern University's travel website:

http://www.it.northwestern.edu/security/travel.html

North Dakota State University's ITS website on traveling abroad with electronic devices:

http://www.ndsu.edu/its/security/traveling_abroad_with_electronic_devices/

Michigan (links to four pages of good advice):

http://global.umich.edu/going-abroad/planning/mobile-computing-guidelines-for-traveling-abroad/

Traveling to China or Russia:

http://pages.uoregon.edu/joe/china-russia/cyber-risks-china-russia.pdf

Working with the ECPOC well ahead of your international trip is the best way to ensure that your travel, items, and information can be taken abroad without a license or violation of the export control laws and/or regulations.

5.9 International Shipping

Most items, as well as some software and information, are subject to U.S. export controls. The impact of these controls on a particular shipment depends on the item, the country it's being shipped to, the entity or individual who will receive it, and the intended end use. There are additional U.S. restrictions on transactions — including but not limited to shipping — with certain countries, entities, and individuals. The fundamental research exception does not apply to physical shipments from the United States. When you export samples, equipment, or instruments abroad or take equipment or instruments with you on an airplane, ship, or boat to attend a conference or conduct research internationally, you are effectively exporting and are subject to certain restrictions and procedures. It is typically not what you know but what you don't know that will delay customs clearance and can ultimately cost hundreds of thousands in export fines and penalties. In addition, most export violations or customs delays are unnecessary and caused by lack of information and preparation.

When exporting from the United States, make sure to verify the import and paperwork requirements in the destination country to ensure smooth customs clearance. You need to allow sufficient time for export processing and license determination. You should start by determining whether you need an

export license to export your equipment/instrument/materials from the United States and help the University secure such license. It may take several months to process a license application.

FSU is the shipper of record, responsible for shipping correctly, and getting the paperwork right. FedEx, UPS, DHL, or a freight forwarder may help or offer advice, and they record the shipment in the government's Automated Export System, but if there's a problem, it's FSU's problem, not theirs.

Some items are hazardous, and need to be packaged and labeled appropriately:

- Biologicals
- Chemicals
- Batteries and fuel cells
- Radioactive materials

Bear in mind that every export from the U.S. is an import somewhere else — your shipment will need to go through Customs in the destination country. Some items may be prohibited or require prior authorization. Some items may incur duty or VAT costs. There are several ways to find the import requirements of the destination country. You can start with the receiving party who should be able to contact their local customs authorities or a customs broker to verify what documents will be needed to clear the shipment through customs. In addition, FedEx has a list of country import requirements on their website which can be helpful in determining import restrictions abroad: http://www.fedex.com/us/international-resource-center/profiles.html.

Exercise judgment when delegating any of the shipping and classification duties to a freight forwarder. Their business is to move freight and not to classify products and determine export license requirements. You should always know what it is that you export and determine whether you need an export license.

FSU requires that individuals responsible for shipping and/or receiving research materials must evaluate, for export control purposes, all items and associated documentation which are intended to be sent to foreign destinations.

The individual handling shipping and/or receiving is the final "gatekeeper" on all controlled outbound shipments from an anti-diversion standpoint. [3] Therefore, it is critical this individual understands the scope of the proposed export and has at his/her disposal all available information in the file (such as screening records and, where applicable, a copy of the export license) in which to make an independent judgment as to the compliance of the export. It is best practice for the individual shipping or receiving an item to double check the terms and conditions of a license against the ship-to instructions associated with a proposed export.

Likewise, when FSU receives items into inventory, certain regulatory requirements (customs and export controls) must be anticipated. For example, when an ITAR item is imported, the item will need to be handled consistent with ITAR physical security access restrictions.

For assistance with export compliance related to the shipping/receiving function, please contact the ECPOC.

5.10 Recordkeeping

This subsection addresses the process for required record retention, as well as where and how records are maintained in accordance with the export regulations.

FSU must comply with regulatory requirements regarding export control-related recordkeeping. These records must be organized so as to be available when requested by U.S. governmental authorities. Records include printed and hard copy documents, as well as electronic records (including e-mail, e-mail attachments, and other electronic files).

All records must be retained for a minimum period of five (5) years from the date of export or from the date of license expiration, as per the requirements of ITAR Section 123.22 and EAR Section 762.6. In some cases, such records will require restricted access where, for example, they contain controlled technical data as part of the transaction.

Examples of records to be retained and desired storage sites are:

Documents	**Storage Site**
MOUs/MOAs/MTAs/NDAs	Office of Research Legal Counsel
Classification and jurisdiction determinations	Department files, ECPOC
License-related documentation	Department files, ECPOC
Screening records	Department files, ECPOC
End user statements	Department files, ECPOC
Sponsored research evaluations	SRA/FSURF, ECPOC
U.S. government communications	Department files, ECPOC, Office of Research Legal Counsel, SRA/FSURF
Shipping and receiving records	Department files, ECPOC

5.11 Issue Reporting and Notification

This subsection addresses the process for confidentially reporting suspected export control violations.

FSU must make every effort to identify suspected or actual violations that occur in conjunction with its export activities. All known or suspected export compliance problems must be documented. Every instance of a suspected violation must be reviewed by the ECPOC. All export shipments and releases of technical data related to the suspected issue must be placed on hold until otherwise authorized by the ECPOC. ECPOC shall escalate compliance issues to the Office of Research Legal Counsel as appropriate and consider Voluntary Disclosure to the relevant agency, as applicable.

Timeliness of reporting is a key issue, since export violations are evaluated not only in terms of their content, but also frequency of occurrence and system-wide implication. Consideration should be given to how and when the Office of Research Legal Counsel authorizes an investigative process to ensure Attorney Client Privilege.

See also subsection 1.7, Voluntary Self-Disclosure of Suspected Violations.

Suspected export control violations may be reported through FSU's Ethics & Compliance Point hotline by calling toll-free (855) 231-7511 (24 hours a day, 365 days a year).

5.12 Export Control Training (Updated 08/10/17)

Research activities conducted by faculty, staff, and students at FSU must be conducted in an ethical and responsible manner following applicable federal or other governmental requirements, sponsor requirements, and University policies and procedures. The Office of Research subscribes to the Collaborative Institutional Training Initiative (CITI Program) offered by the University of Miami. CITI's web-based training materials serve millions of learners at academic institutions, government agencies, and commercial organizations in the U.S. and around the world.

CITI's Export Compliance course includes an introduction to export compliance as well as information focused on export compliance as it relates to biosafety, operational departments, international shipping, purchasing, international and foreign waters, collaborations, and U.S. sanctions programs, distance education, and technology. It is designed for use by investigators, members of the research team, key personnel across operational departments, and others who work with or may be responsible for federally controlled devices, materials, or technologies.

Information on accessing this free course on export controls may be found here.

5.13 Start-up and Spin-off Activity

This subsection addresses start-up and similar spin-off companies that are initiated by FSU faculty members, separate from FSU-employed research and administration. FSU encourages such activity both as a means for transferring technology and for local economic development. FSU's Office of Commercialization staff will help a researcher determine the feasibility of establishing such a venture, provide general business advice, assist modestly with a business plan, recommend financing options, facilitate the licensing process, and close deals in a timely manner.

It is important to note that the use of FSU's laboratories and resources for any activity other than fundamental research could trigger export control requirements that FSU would not otherwise be aware of or accept as part of its compliance risk. Hence, it is important that the directors and administrators of start-ups or spin-off businesses and entities (who may in parallel hold teaching and research positions at FSU) be aware that, per FSU's policy, all such *proprietary* activities must be performed separately from FSU's own and dedicated research laboratory space. This also includes proprietary consulting arrangements that faculty members may have.

5.14 Monitoring and Auditing

In order to maintain FSU's export compliance program and ensure consistent adherence to U.S. export laws, the ECPOC may periodically conduct internal reviews of TCPs and certain projects. The purpose of the review is to identify possible violations and/or deficiencies in training, procedures, etc., that can be rectified. If a violation or non-compliance is detected, the ECPOC, in consultation with the Research Legal Counsel and/or VPR as needed, will develop a plan to follow up and implement corrective actions.

5.15 Disciplinary Actions

In recognition of the seriousness of non-compliance with export controls, FSU will address non-compliance in accordance with the FSU policies and procedures. Further, all FSU employees responsible for export controls compliance or participating in export-controlled projects must be aware of the substantial criminal and civil penalties imposed by the Federal government for violation of the export regulations including personal liability, monetary fines, and imprisonment. See subsection 1.5, Penalties for Export Violations, for additional information.

5.16 Employee Protection

In accordance with the FSU Policies, no individual shall be punished solely because he or she reported what was reasonably believed to be an act of wrongdoing or export control violation. However, a FSU employee may be subject to disciplinary action if the employee knowingly fabricated, knowingly distorted, or knowingly exaggerated the report. See the following notice regarding whistleblower protection: Federal Pilot Program for Enhancement of Employee Protection from Reprisal for Disclosure of Certain Information. See also 4-OP-C-13, Policy against Fraudulent, Unethical and Other Dishonest Acts.

SECTION 6 - Additional Information

6.1 Acronyms

Term	Meaning
AECA	Arms Export Control Act
BIS	Bureau of Industry and Security
CAU	Custody, Access and Use Agreement
CCL	Commerce Control List
CFR	Code of Federal Regulations
DDTC	Directorate of Defense Trade Controls
DoC	U.S. Department of Commerce
DoS	U.S. Department of State
DoT	U.S. Department of the Treasury
EAA	Export Administration Act
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
ECO	Export Control Officer
FACR	Foreign Assets Control Regulations
FSO	Facility Security Officer
FSU	Florida State University
FSURF	FSU Research Foundation
ITAR	International Traffic in Arms Regulations
MOU	Memorandum of Understanding
NISPOM	National Industrial Security Program Manual
OFAC	Office of Foreign Assets Control

Term	Meaning
OC	Office of Commercialization
ECPOC	Office of Research Compliance Programs
PI	Principal Investigator
SRA	Sponsored Research Administration
TCP	Technology Control Plan
USML	U.S. Munitions List
VPR	FSU Vice President for Research

6.2 Disclaimer

The FSU Export Controls Compliance Program, Guidelines, Technology Control Plan, process, and other materials are specifically tailored to the FSU research community. This instruction and all other materials therein are not intended to replace any regulatory document of interpretation or to relieve importers or exporters of their statutory responsibility to comply with current laws, regulations, policies, and procedures of the U.S. Government. FSU's export control content may not apply to other specific situations that occur outside of the FSU research community or may be incomplete. FSU's export control materials do not constitute legal advice. Those outside of the FSU research community should not act or rely on any of this information and should seek the advice of an attorney before taking any actions.

6.3 Acknowledgements

Florida State University (FSU) acknowledges and appreciates the University of Chicago, the University of Arizona, Virginia Polytechnic Institute and State University, and the University of Florida for granting FSU permission to alter selected portions of their export control program guidelines for use in this Plan.

6.4 References

Export Administration Regulations, 15 CFR 730-774
International Traffic in Arms Regulations, 22 CFR 120-130
Office of Foreign Assets Control, 31 CFR 500-598
FSU Export Control Policy
Fla. Stat. 1004.22, Divisions of Sponsored Research at State Universities

[1] Other affected temporary visa categories include B1, L1, and O.

[2] For example, under ITAR Part 126.1, China is a proscribed country for which DDTC will not issue an ITAR license; this prohibition and presumption of license denial extends to Chinese foreign nationals for whom ITAR items remain absolutely restricted

[3] Anti-diversion: The United States Bureau of Export Administration requires all exports to be shipped with a destination control statement that states the destination of the exported goods, and the law prohibits the goods from being diverted to any other destination.