THE PENNSYLVANIA STATE UNIVERSITY

EXPORT COMPLIANCE PROCEDURE MANUAL

List of Abbreviations

AVP: DOTM	Associate Vice President, Director of Office of Technology Management
DSOP	Director in Office of Sponsored Programs
BIS	Department of Commerce Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
DDTC	Department of State Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
CEC:OSP	Chair Export Control Compliance Committee in Office of Sponsored Programs
ITAR	International Traffic in Arms Regulations
OFAC	Department of the Treasury Office of Foreign Assets Control
OSP	Office of Sponsored Programs
PI	Principal Investigator
SDN List	Specially Designated Nationals and Blocked Persons List
SSL	Secure Sockets Layer
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List
Penn State	Pennsylvania State University
VPN	Virtual Private Network

TABLE OF CONTENTS

OVERVIEW OF EXPORT CONTROLS

I. INTRODUCTION

The U.S. export control system generally requires export licensing for defense items, for items that have both commercial and military applications, and for exports to sanctioned persons and destinations. U.S. national security, economic interests and foreign policy shape the U.S. export control regime. The export laws and regulations aim at achieving various objectives, such as preventing the proliferation of weapons of mass destruction, advancing the U.S. economic interests at home and abroad, protecting the U.S. strategic superiority/interests, aiding regional stability, implementing anti-terrorism and crime controls, and protecting human rights.

These controls generally restrict the export of products and services based on the type of product and the destination of the export. In both the defense and high-technology sectors, the U.S. Government tightly regulates the export not only of equipment and components, but also of technology. Technology includes technical data, such as blueprints and manuals, as well as design services (including the transfer of "knowledge") and training. U.S. laws assert jurisdiction over U.S.-origin equipment and technology even after it is exported (*i.e.*, restricting the re-export or re-transfer to third parties). In addition to general export licensing, the United States cooperates in/complies with United Nations embargoes and maintains its own economic embargoes against a number of countries whose governments consistently violate human rights or act in support of global terrorism. Such embargoes bar most transactions by U.S. persons with these countries.

Three principal agencies regulate exports from the United States: the U.S. Department of State Directorate of Defense Trade Controls ("DDTC") administers export control of defense exports; the U.S. Department of Commerce Bureau of Industry and Security ("BIS") administers export control of so-called "dual-use" technologies; and the U.S. Department of the Treasury Office of Foreign Assets Control ("OFAC") administers exports to embargoed countries and designated entities.

Penn State has a policy covering export control issues (RA18) as well as guidelines (RAG11) that provide additional guidance on export matters.

II. EXPORT CONTROLS AND UNIVERSITY RESEARCH

U.S. national security and economic interests are heavily dependent on technological innovation and advantage. Many of the nation's leading-edge technologies, including defense-related technologies, are being discovered by U.S. and foreign national students and scholars in U.S. university research and university-affiliated laboratories. U.S. policymakers recognize that foreign students and researchers have made substantial contributions to U.S. research efforts, but the potential transfer of controlled defense or dual-use technologies to their home countries could have significant consequences for U.S. national interests. The U.S. export control agencies place the onus on universities to understand and comply with the regulations.[1]

Export controls present unique challenges to universities and colleges because they require balancing concerns about national security and U.S. economic vitality with traditional concepts of unrestricted academic

[1] *See* GAO Report "Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities," December 2006, available at http://www.gao.gov/new.items/d0770.pdf.

freedom, and publication and dissemination of research findings and results. University researchers and administrators need to be aware that these laws may apply to research, whether sponsored or not. However, it also is important to understand the extent to which the regulations do not affect normal university activities.

III. EXPORT OF DEFENSE ARTICLES AND SERVICES – INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

Under the International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130,[2] DDTC administers the export and re-export of defense articles, defense services and related technical data from the United States to any foreign destination, or to any foreign person, whether located in the United States or abroad. Section 121.1 of the ITAR contains the *United States Munitions List* ("USML") and includes the commodities and related technical data and defense services controlled for export purposes. The ITAR controls not only end items, such as radar and communications systems, military encryption and associated equipment, but also the parts and components that are incorporated into the end item. Certain non-military items, such as commercial satellites, and certain chemical precursors, toxins, and biological agents, are also controlled.

A. ITEMS CONTROLLED UNDER THE ITAR

The ITAR uses three different terms to designate export controlled items – defense articles, technical data, and defense services. With rare exceptions, if an item contains any components that are controlled under the ITAR, the entire item is controlled under the ITAR. For example, a commercial radio that would normally not be controlled under the ITAR becomes a controlled defense article if it contains an ITAR-controlled microchip.

1. Defense Article means any item or technical data that is specifically designed, developed, configured, adapted, or modified for a military, missile, satellite, or other controlled use listed on the USML.[3] Defense article also includes models, mock-ups, or other items that reveal technical data relating to items designated in the USML.

2. Technical Data means any information for the design, development, assembly, production, operation, repair, testing, maintenance, or modification of a defense article. Technical data may include drawings or assembly instructions, operations and maintenance manuals, and email or telephone exchanges where such information is discussed. However, technical data does not include general scientific, mathematical, or engineering principles commonly taught in schools, information present in the public domain, general system descriptions, or basic marketing information on function or purpose.[4]

3. Defense Service means providing assistance, including training, to a foreign person in the United States or abroad in the design, manufacture, repair, or operation of a defense article, as well as providing technical data to foreign persons. Defense services also include informal collaboration, conversations, or interchanges concerning technical data.[5]

---

[2] The ITAR are promulgated pursuant to Section 38 of the Arms Export Control Act, 22 U.S.C. §§ 2778 *et seq*.

[3] 22 C.F.R. § 120.6.

[4] 22 C.F.R. § 120.10. Note that the ITAR uses the term "blueprints" to cover drawings and assembly instructions.

[5] 22 C.F.R. § 120.9.

B. THE USML CATEGORIES

The USML designates particular categories and types of equipment as defense articles and associated technical data and defense services.[6] The USML divides defense items into 21 categories, listed below. 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/ITAR_Part_121.pdf.

I	Firearms, Close Assault Weapons and Combat Shotguns
II	Guns and Armament
III	Ammunition / Ordnance
IV	Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
V	Explosives, Propellants, Incendiary Agents, and their Constituents
VI	Vessels of War and Special Naval Equipment
VII	Tanks and Military Vehicles
VIII	Aircraft and Associated Equipment
IX	Military Training Equipment
X	Protective Personnel Equipment
XI	Military Electronics
XII	Fire Control, Range Finder, Optical and Guidance and Control Equipment
XIII	Auxiliary Military Equipment
XIV	Toxicological Agents and Equipment and Radiological Equipment
XV	Spacecraft Systems and Associated Equipment
XVI	Nuclear Weapons, Design and Testing Related Items
XVII	Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
XVIII	Directed Energy Weapons
XIX	[Reserved]
XX	Submersible Vessels, Oceanographic and Associated Equipment
XXI	Miscellaneous Articles

C. CLASSIFICATION

While DDTC has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify the item. If doubt exists as to whether an article or service is covered by the USML, upon written request in the form of a Commodity Jurisdiction ("CJ") request, DDTC will provide advice as to whether a particular article is a defense article subject to the ITAR, or a dual-use item subject to Commerce Department licensing.[7] Determinations are based on the origin of the technology (*i.e.*, as a civil or military article), and whether it is predominantly used in civil or military applications. University employees should

[6] *See* 22 C.F.R. § 121.1.

[7] *See* 22 C.F.R. § 120.4. Note that DDTC has jurisdiction over determining whether an item is ITAR- or EAR-controlled. While BIS at Commerce provides assistance with determining the specific ECCN of a dual-use item listed on the CCL, if doubt exists as to whether an item is ITAR- or EAR-controlled, BIS will stay its classification proceeding and forward the issue to DDTC for jurisdiction determination.

contact the Export Compliance Officer in the Office of Sponsored Programs ("ECO:OSP") when classifying an item. If The Pennsylvania State University ("PSU") needs to obtain a CJ determination, the ECO:OSP in conjunction with PSU legal counsel and PSU's Empowered Official will file the CJ request with DDTC.[8]

D. 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."[9] The following are examples of exports:

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

- 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, including data, 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.

E. AUTHORIZATION TO EXPORT

Generally, any U.S. person or entity that manufactures, brokers, or exports defense articles or services must be registered with DDTC.[10] Registration is required prior to applying for a license or taking advantage of any license exemption.[11] Once the registration is complete, an exporter may apply for an export authorization by submitting a relatively simple license application for the export of defense articles or technical data; or a complex license application, usually in the form of a Technical Assistance Agreement ("TAA"), for a complex transaction that will require the U.S. entity to provide defense services. Most types of applications also contain

[8] Instructions on the content of a CJ and the filing procedure are available at: http://www.pmddtc.state.gov/commodity_jurisdiction/index.html

[9] 22 C.F.R. § 120.17.

[10] 22 C.F.R. § 122.1.

[11] 22 C.F.R. §§ 120.1(c) and (d); 122.1(c).

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.

The University is registered with the DDTC and renews its registration annually, therefore, faculty are not required to register with the DDTC for university research. [12] University researchers are usually engaged only in the creation of technical data that is not subject to ITAR or EAR, and are engaged primarily in the fabrication of articles for experimental or scientific purposes, including research and development. No license is needed if only U.S. Persons are involved or have access to defense articles or defense technology.

However, if the University desires to involve foreign nationals in ITAR-controlled research, it must register with the DDTC to apply for a license or take advantage of certain license exemptions. For these reasons, the University regularly reviews projects and available license exemptions to determine of a license is required. License exemptions specific to universities, as well as licensing procedures, are described in detail in the *Key Issues in University Research* section on page 19.

F. EMBARGOED COUNTRIES UNDER DDTC REGULATIONS

ITAR Prohibitions. In general, no ITAR exports may be made either under license or license exemption to countries proscribed in 22 C.F.R. § 126.1, such as Cuba, Eritrea, Iran, North Korea, Syria and Venezuela. 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

IV. EXPORT OF COMMERCIAL DUAL-USE GOODS AND TECHNOLOGY – EXPORT ADMINISTRATION REGULATIONS

The Department of Commerce Bureau of Industry and Security ("BIS") regulates the export of commercial products and technology under the Export Administration Regulations, 15 C.F.R. §§ 730-774 ("EAR"). [13] While there are some parallels to the ITAR, there also are some major differences in how the regulations and the relevant agencies function.

They are similar in that both agencies focus on "technology transfer" and have been increasingly focused on enforcement. They differ in that the EAR covers a wider range of products and technology, the product classification process is highly technical, and most importantly, the need for a license depends not only on the type of product but on its final destination.

A. ITEMS CONTROLLED UNDER THE EAR

Generally, all items of U.S.-origin, or physically located in the United States, are subject to the EAR. Foreign manufactured goods are generally exempt from the EAR re-export requirements if they contain less

[12] *See* 22 C.F.R. §§ 122.1(b)(3) and (b)(4).

[13] The EAR are promulgated under the Export Administration Act of 1979, as amended (50 U.S.C. app. §§ 2401-2420). From August 21, 1994, through November 12, 2000, the Act was in lapse. During that period, the President, through Executive Order 12924, which had been extended by successive Presidential Notices, continued the EAR in effect under the International Emergency Economic Powers Act (50 U.S.C. §§ 1701-1706 (IEEPA). On November 13, 2000, the Act was reauthorized by Pub. L. No. 106-508 (114 Stat. 2360 (2000)) and it remained in effect through August 20, 2001. Since August 21, 2001, the Act has been in lapse and the President, through Executive Order 13222 of August 17, 2001, which has been extended by successive Presidential Notices, has continued the EAR in effect under IEEPA.

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.[14] The following summarizes the types of items controlled under the EAR:

- **Commodities**. This includes finished or unfinished goods ranging from high-end microprocessors to airplanes, to ball bearings.
- **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**. Technology, as defined in the EAR, includes both technical data, and services. 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.

B. THE COMMERCE CONTROL LIST CATEGORIES

The CCL provides a list of very specific items that are controlled. The CCL is divided into the nine categories below. The CCL is available online at http://www.access.gpo.gov/bis/ear/ear_data.html.

CATEGORIES

0.		Nuclear Materials, Facilities & Equipment (and Miscellaneous items)
1.		Materials, Chemicals, Microorganisms and Toxins
2.		Materials Processing
3.		Electronics
4.		Computers
5.	pt-1	Telecommunications
5.	pt-2	Information Security (encryption)
6.		Sensors & Lasers
7.		Navigation and Avionics
8.		Marine (vessels, propulsion, and equipment)

[14] 15 C.F.R. § 734.

9. Propulsion systems, Space Vehicles (includes aircraft & aircraft engines)

C. CLASSIFICATION

As discussed in *Overview*, Section III.C, DDTC 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.[15]

Once it is determined that an item is EAR-controlled, the exporter must determine its Export Control Classification Number ("ECCN"). BIS has two assistance procedures where the proper ECCN classification or licensing requirements are uncertain.[16] To determine EAR's applicability and the appropriate ECCN for a particular item, a party can submit a "Classification Request" to BIS. To determine whether a license is required or would be granted for a particular transaction, a party can request BIS provide a non-binding "advisory opinion." While BIS provides assistance with determining the specific ECCN of a dual-use item listed on the CCL, if doubt exists as to whether an item is ITAR- or EAR-controlled, BIS will stay its classification proceeding and forward the issue to DDTC for jurisdiction determination.

Unlike the ITAR, for classification purposes BIS generally looks at the classification of the complete product being exported rather than at the classification of each subcomponent of the item (*i.e.*, "black box" treatment, as opposed to the "see through" treatment under the ITAR).

D. DEFINITION OF EXPORT AND RE-EXPORT UNDER THE EAR

1. Export. Export is defined as the actual shipment or transmission of items subject to the EAR out of the United States. The EAR is similar to the ITAR in that it covers intangible exports of "technology," including source code, as well as physical exports of items.

2. Deemed Export. Under the EAR the release of technology to a foreign national in the United States is "deemed" to be an export, even though the release took place within the United States. 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.

3. Re-export. Similarly to the ITAR, the EAR attempts to impose restrictions on the re-export of U.S. goods, *i.e.*, the shipment or transfer to a third country of goods or technology originally exported from the United States.

4. Deemed Re-export. Finally, the EAR defines "deemed" re-exports as the release of technology by a foreign national who has been licensed to receive it to the national of another foreign country who has not been licensed to receive the technology. For example, ECCN 5E001 technology may be exported to a university in Ireland under the license exception for technology and software, but might require a deemed re-export license authorization before being released to a Russian foreign national student or employee of that university in Ireland.

[15] For a complete discussion, *see Overview of Export Controls*, Section III.C
[16] *See* 15 C.F.R. § 748.3.

E. AUTHORIZATION TO EXPORT

Once it has been determined that a license is required, an exporter can apply for export authorization from BIS. Unlike the ITAR, there is no requirement for formal registration prior to applying for export authorization. Additionally, the EAR has no equivalent to the TAA used in ITAR exports.

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.[17]

Each category of the CCL contains ECCNs for specific items divided into five categories, A through E: "A" refers to specific systems or equipment (and components); "B" refers to test, inspection and production equipment; "C" refers to materials; "D" refers to software; and "E" refers to the technology related to that specific equipment. For example, most civil computers would be classified under ECCN 4A994. The "4" refers to Category 4, *Computers*, and the "A" refers to the subcategory, *i.e.*, equipment. Generally, if the last three digits begin with a 'zero' or 'one' (*e.g.*, 4A001), the product is subject to stringent controls, whereas if the last three digits are a "9XX" (*e.g.*, 4A994), then generally there are fewer restrictions on export.

Once an item has been classified under a particular ECCN, a person can determine whether a license is required for export to a particular country. The starting place is the information following the ECCN heading. The "List of Items Controlled" describes the specific items covered or not covered by the ECCN.

(1) *Determine Reason for Controls.* The "License Requirements" section provides notations as to the reasons for control. These reasons include:

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 Security
SS	Short Supply	XP	Computers
SI	Significant Items		

The most commonly used controls are Anti-Terrorism and National Security, while other controls only apply to limited types of articles. For example, ECCN 4A994 lists “License Requirements: Reason for Control: AT” (*i.e.*, anti-terrorism) and the following:

Control(s)	Country Chart
AT applies to entire entry	AT Column 1

(2) *Apply Country Chart*. Once an item is identified as meeting the criteria for a particular ECCN, the user can refer to the chart found at 15 C.F.R. § 738, Supp. 1. If the particular control applies to that country, a license is required. For example, Syria has an “X” under AT Column 1, therefore a license would be required unless an exception applied.

[17] 15 C.F.R. § 740.

(3) *Exceptions*. 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. These exceptions include:

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.
CTP	Computer exports to certain countries.
KMI	Encryption exemption for key management.
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.
GFT	Certain gifts and humanitarian donations.
GOV	Exports to certain government entities.
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.

License exceptions specific to universities, as well as licensing procedures, are described in detail in *Key Issues in University Research*.

V. OFAC SANCTIONS PROGRAM AND BARRED ENTITIES LISTS

A. LIST OF SANCTIONED COUNTRIES UNDER OFAC REGULATIONS

U.S. economic sanctions broadly prohibit most transactions between a U.S. person and persons or entities in an embargoed country which are currently: Cuba, Iran, North Korea, Syria, and Sudan.[18] This prohibition includes importation and exportation of goods and services, whether direct or indirect, as well as "facilitation" by a U.S. person of transactions between foreign parties and a sanctioned country. More limited sanctions may block particular transactions or require licenses under certain circumstances for exports to a number of countries, currently including but not limited to Burma, Liberia, and Zimbabwe.[19] Because this list is not complete and subject to change, please visit:

http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

While most sanctions are administered by OFAC, BIS has jurisdiction over certain exports prohibitions (via "embargo" regulations), as is the case with exports to Syria. [20] Economic sanctions and embargo programs are country-specific and very detailed in the specific prohibitions.

B. EMBARGOED COUNTRIES

In addition to countries barred by the Treasury Department under OFAC, the department of state also maintains a list of embargoed countries. As stated previously, as a general rule, no ITAR exports may be made either under license or license exemption to countries proscribed in 22 C.F.R. § 126.1, such as Cuba, Eritrea, Iran, North Korea, Syria and Venezuela. 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. While China is not technically on an embargoed country list, members of the University community should be aware that it is difficult to obtain the necessary permissions to export to China both under the EAR and ITAR.

C. TERRORIST AND OTHER BARRED ENTITY LISTS

Various U.S. Government agencies maintain a number of lists of individuals or entities barred or otherwise restricted from entering into certain types of transactions with U.S. persons. Such lists must be screened to ensure that the university does not engage in a transaction with a barred entity. Penn State has a limited license to use Visual Compliance™ to expedite screening of these and other lists.

- **Specially Designated Nationals and Blocked Persons List ("SDN List")**. Maintained by OFAC, this is a list of barred terrorists, narcotics traffickers, and persons and entities associated with embargoed regimes. Generally, all transactions with such persons are barred. The *SDN List* is available at: http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml.

[18] With the exception of the sanctions on Cuba and North Korea, OFAC sanctions are promulgated under the International Emergency Economic Powers Act of 1977, 50 U.S.C. §§ 1701-1706 (IEEPA). The embargoes on Cuba and North Korea are promulgated under the Trading with the Enemy Act of 1917, 12 U.S.C. § 95a (TWEA).

[19] *See* http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx for a full list of U.S. sanction programs.

[20] *See* 15 C.F.R. § 746.

- **Persons Named in General Orders (15 C.F.R. § 746, Supp. No. 9).** General Order No. 2 contains the provisions of the U.S. embargo on Syria.. A link to the General Orders is available at: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ba2d5996d28cc22033ea2bfb857555cc&rgn=div5&view=text&node=15:2.1.3.4.30&idno=15

- **List of Debarred Parties**. The Department of State bars certain persons and entities from engaging in the export or re-export of items subject to the USML (available at: http://www.pmddtc.state.gov/compliance/debar.html). Note that the number of countries subject to a U.S. arms embargo is much broader than those subject to OFAC embargoes. *See* http://www.pmddtc.state.gov/embargoed_countries/index.html.

- **Denied Persons List**. These are individuals and entities that have had their export privileges revoked or suspended by BIS. The *Denied Persons List* is available at: http://www.bis.doc.gov/dpl/Default.shtm.

- **Entity List**. These are entities identified as being involved in proliferation of missile technology, weapons of mass destruction, and related technologies. The *Entity List* is available at: http://www.bis.doc.gov/Entities/Default.htm.

- **Unverified List**. These are foreign persons and entities for which BIS has been unable to verify the nature of their operations. While transactions with these entities are not barred, special due diligence is required. The *Unverified List* is available at: http://www.bis.doc.gov/Enforcement/UnverifiedList/unverified_parties.html.

- **Excluded Parties List**. These are entities that have been barred from contracting with U.S. Government agencies. In general, companies cannot contract with such parties in fulfilling a U.S. Government contract, either as prime or sub-contractor. The *EPLS* is available at: http://www.epls.gov/.

- **Nonproliferation Sanctions.** These are maintained by the Department of State. These lists are available at: http://www.state.gov/t/isn/c15231.htm.

VI. ANTI-BOYCOTT RESTRICTIONS

The anti-boycott rules were implemented to prevent U.S. business from participating directly or indirectly in the Arab League's boycott of Israel. The laws prevent U.S. persons from doing business under terms that would restrict that person's ability to do business with other countries under a boycott not recognized by the U.S. The Arab League's boycott has lessened over the years, but still remains in effect in some countries. These restrictions are enforced by BIS. The applicable regulations are at 15 C.F.R. § 760.

Anti-boycott restrictions are most likely to appear in dealings with entities in certain Arab League countries. As of this writing, Bahrain, Bangladesh, Iraq, Kuwait, Lebanon, Libya, Oman, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen continue to impose boycott restrictions on Israel and companies that do business with Israel. Iraq is not included in this list, but its status with respect to the future lists remains under review by the Department of Treasury.[21] Egypt and Jordan have ceased participating in the boycott.

http://www.bis.doc.gov/antiboycottcompliance/oacantiboycottrequestexamples.html

[21] *See* Department of Treasury List of Countries Requiring Cooperation with an International Boycott, 72 Fed. Reg. 60930 (Oct. 26, 2007).

Note that there are strict reporting requirements even where the U.S. person refuses to participate in a requested boycott action. In other words, if we are asked to participate in a boycott of Israel and we refuse, we still have to report to the U.S. Government that we were asked.

A. JURISDICTION

These laws generally apply to any person or entity in the U.S., and to U.S. persons or entities abroad. As examples, the laws apply to:

- A foreign company's affiliate or permanent office in the U.S.
- A U.S. company's foreign affiliate's transaction with a third-party if that affiliate is controlled by the U.S.company and involves shipment of goods to or from the U.S.

B. RED FLAGS

The Commerce Department has set forth the following red flags to look for as signs of anti-boycott restrictions:

- Agreements to refuse or actual refusals to do business with Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin, or nationality.
- Furnishing information about business relationships with Israel or with blacklisted companies.
- Furnishing information about the race, religion, sex, or national origin of another person.
- Paying or otherwise implementing letters of credit that include requirements to take boycott-related actions prohibited by the anti-boycott regulations.

These restrictions may appear on pre-printed portions of agreements.

C. EXCEPTION

A major exception to the anti-boycott rules is the provision that permits compliance with the import requirements of a boycotting country. This exception permits firms to comply with import restrictions that prohibit imports from Israel or Israeli firms. The exception does not permit compliance with a boycott of blacklisted firms outside of Israel, nor does it allow for the issuance of a negative certificate-of-origin of any type. Other exceptions allow firms to provide country-of-origin information on the shipping documents, or information required for immigration or employment purposes. The exceptions can be found at 15 C.F.R. § 760.3.

D. REPORTING

Any U.S. person or entity who is asked to enter into an agreement or provide information that would violate anti-boycott laws must report this to BIS using a form BIS-621-P in accordance with 15 C.F.R. § 760.5. Information regarding the reporting of suspected anti-boycott activities can be found at

http://www.bis.doc.gov/ComplianceAndEnforcement/index.htm. In addition, the U.S. Internal Revenue Service (IRS) requires U.S. taxpayers to report operations in or relating to boycotting countries and nationals and request to cooperate with boycott activities. *See* IRS Form 5713, located online at: http://www.irs.gov/pub/irs-pdf/f5713.pdf.

These reporting requirements apply even where the U.S. person or entity refuses to participate. Crossing out the boycott language in a proposed contract does not end the matter. The duty to report remains even where the requesting foreign entity accepts the redaction of the boycott language.

For more information on anti-boycott rules see: http://www.bis.doc.gov/complianceandenforcement/antiboycottcompliance.htm. The Office of Boycott Compliance has also set up an advice line for questions about the anti-boycott rules, which can be reached at (202) 482-2381.

VII. PENALTIES FOR EXPORT VIOLATIONS

A. GENERAL OVERVIEW

Generally, any person or entity that brokers, exports, or attempts to export a controlled item without prior authorizationor in violation of the terms of a license, is subject to penalties. Violators may incur both criminal and civil penalties. Although there is a maximum amount for a civil or criminal penalty, the actual penalty imposed is often multiplied. For instance, each shipment might be considered a separate violation, and BIS will often find multiple violations of related restrictions in connection to each shipment (*e.g.*, export without a license, false representation, actions with knowledge of a violation, *etc*.). A series of violations occurring over a period of time may result in hundreds of thousand or even millions of dollars of penalties.

B. DEFENSE EXPORTS

The Arms Export Controls Act and the ITAR provide that wilful violations of the defense controls can be fined up to $1,000,000 per violation, or twenty years of imprisonment, or both.[22] In addition, the Secretary of State may assess civil penalties, which may not exceed $500,000 per violation.[23] The civil penalties may be imposed either in addition to, or in lieu of, any other liability or penalty. Penalties may be imposed on the individual and/or the employer. The articles exported or imported in violation, and any vessel, vehicle or aircraft involved in such attempt is subject to seizure, forfeiture and disposition.[24] Finally, the Assistant Secretary for Political-Military Affairs may order debarment of the violator, *i.e.*, prohibit the violator from participating in export of defense items.[25]

While imposing criminal liability is fairly rare, many major U.S. companies and some U.S. universities have been assessed significant civil penalties in the millions of dollars.[26] For example, an investigation into the

[22] 22 U.S.C. § 2778(c) and 22 C.F.R. § 127.3.

[23] 22 U.S.C. § 2778(e) and 22 C.F.R. § 127.10.

[24] 22 C.F.R. § 127.6.

[25] 22 U.S.C. § 2778(g) and 22 C.F.R. § 127.7.

[26] For a thorough discussion of penalties imposed under the ITAR, *see* John C. Pisa-Relli, "Monograph on U.S. Defense Trade Enforcement" (February 2007).

research of Dr. J. Reece Roth, emeritus faculty member at the University of Tennessee at Knoxville, on a U.S. Air Force project to develop plasma actuators that could be used to control the flight of small, subsonic, unmanned, military drone aircraft. Dr. Roth was convicted by a federal jury on one count of conspiracy, fifteen counts of exporting defense articles and services without a license, and one count of wire fraud for allowing research assistants from China and Iran to access sensitive data, taking sensitive documents to China as well as emailing sensitive information to China. He is currently serving a 4 year prison sentence. The case marked the first time the government used the act to crack down on the distribution of restricted data to foreigners in a university setting.[27]

Both DDTC and BIS have stated that they believe that many universities are in violation of the regulations based on the low number of licenses received in relation to the number of foreign students enrolled.

C. DUAL-USE ITEMS EXPORTS AND ANTI-BOYCOTT VIOLATIONS

Similarly to the ITAR, violations of the EAR are subject to both criminal and administrative penalties. Fines for export violations, including anti-boycott violations, can reach up to $1,000,000 per violation in criminal cases, and $500,000 per violation in most administrative cases. In addition, criminal violators may be sentenced to prison time up to 20 years, and administrative penalties may include the denial of export privileges.[28] A denial order is probably the most serious sanction because such order would bar a U.S. company from exporting for a period of years or bar a foreign entity from buying U.S. origin products for such period.

In most instances, BIS reaches negotiated settlements in its administrative cases, as a result of voluntary self-disclosures of violations by companies and individuals. Voluntary disclosures constitute a major mitigating factor in determining penalties, reducing the amount of penalty by up to 50 percent, provided certain conditions are met, such as the implementing of a comprehensive compliance program.[29]

D. EXPORTS TO A SANCTIONED COUNTRY

Although potential penalties for violations of U.S. export laws vary depending on the country and product involved, an exporter may be subject to a maximum civil penalty of $500,000 per violation under

---

[27] *See* Bureau of Political-Military Affairs; Statutory Debarment of ITT Corporation Pursuant to the Arms Export Control Act and the International Traffic in Arms Regulations, 72 Fed. Reg. 18310 (Apr. 11, 2007). For a detailed account of the ITT Corporation investigation, *see* the U.S. Department of Justice press release "ITT Corporation to Pay $100 Million Penalty and Plead Guilty to Illegally Exporting Secret Military Data Overseas" (March 27, 2007), available at: http://www.usdoj.gov/opa/pr/2007/March/07_nsd_192.html.

[28] *See* Bureau of Industry and Security "Don't Let This Happen To You Booklet, An Introduction to U.S. Export Control Law Actual Investigations of Export Control and Anti-boycott Violations", 2010. http://www.bis.doc.gov/complianceandenforcement/dontletthishappentoyou_2010.pdf
See United States of America vs John Reece Roth Court of Appeals, for a detailed account of the investigation, conviction and appeal request. http://www.ca6.uscourts.gov/opinions.pdf/11a0003p-06.pdf

[29] For a review of BIS investigations and penalties, *see* "Don't Let This Happen to You! Actual Investigations of Export Control and Anti-boycott Violations" at: http://www.bis.doc.gov/complianceandenforcement/dontletthishappentoyou-2010.pdf.

OFAC regulations, with the exception of exports to Cuba or North Korea.[30] Violations of the Cuban or North Korean sanctions are subject to a maximum penalty of $55,000 per violation.[31]

The U.S. Government can also seek to criminally prosecute conduct where violations are willful and knowing. Such violations may reach $1,000,000 per violation and imprisonment of up to 20 years. In addition, where there is egregious conduct by the offender, BIS (who assists OFAC in enforcing sanctions) may suspend the export privileges of a company.

In assessing penalties, DDTC, BIS, and OFAC will consider a number of factors, both aggravating and mitigating. Mitigating factors include (1) whether the disclosure was made voluntarily; (2) whether this was a first offense; (3) whether the company had compliance procedures; (4) whether steps were taken to improve compliance after discovery of violations; and (5) whether the incident was due to inadvertence, mistake of fact, or good faith misapplication of the laws. Aggravating factors include: (1) willful or intentional violations; (2) failure to take remedial action after discovery; (3) lack of a compliance program; and (4) deliberate efforts to hide or conceal a violation.

[30] Violations of most of the Economic Sanction Regulations are set under the IEEPA. *See* supra note 30.

[31] The OFAC embargoes of Cuba and North Korea were promulgated under the Trading with the Enemy Act (TWEA).

KEY ISSUES IN UNIVERSITY RESEARCH

I. 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. Though taking place inside the U.S., the transfer is "deemed" to be an export. The term "deemed export" is unique to the EAR.

Both the ITAR and the EAR provide for deemed exports. While the ITAR distinguishes between the transfer of *technical data* and *defense services*, the EAR generally provides for the release of *technology*. Such transfer or release may be made through oral, visual, or other means. An export may occur through:

1. a demonstration;
2. oral briefing;
3. telephone call;
4. leaving voicemail messages;
5. laboratory or plant visit;
6. presenting at conferences and meetings;
7. faxes or letters;
8. hand-carried documents, hardware or drawings;
9. design reviews;
10. the exchange of electronic communication;
11. posting non-public data on the Internet or any local area networks (LAN);
12. carrying a laptop with controlled technical information or software to an overseas destination; or
13. collaborating with other universities/research centers through research efforts.

The issue of deemed exports is particularly relevant to university research because of the activities that normally take place at a university. 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, foreign students' or researchers' involvement may trigger export control compliance issues.

II. U.S. AND FOREIGN PERSONS

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.*, 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).[32] 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.

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

Note that the definitions for a U.S. and a foreign person differ for purposes of the OFAC sanctions.

INFORMATION NOT SUBJECT TO OR EXCLUDED FROM EXPORT CONTROLS

It is important to note that most of the activities that Penn State engages in are fundamental research. As such, most activities are not subject to export controls, or even if controlled, do not require licensing. Both the ITAR and the EAR have special provisions relating to **information** that is not subject to export controls, including limited exclusions regarding the release of information in the context of university research and educational activities. Additionally, the embargo regulations have exceptions for certain information and informational materials.

A. PUBLICLY AVAILABLE

The ITAR and the EAR do not control information which is published and generally accessible or available to the public. Note that even though the two regimes have similar scope, the ITAR and the EAR vary in the specific information that qualifies as publicly available.

- **ITAR provision:** The ITAR describes such information as information in the *public domain*.[33] The information in the public domain may be obtained through:
    - sales at newsstands and bookstores;
    - subscription or purchase without restriction to any individual;
    - second class mailing privileges granted by the U.S. Government; e.g. periodicals and newspapers
    - at libraries open to the public;
    - patents available at any patent office;
    - unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, **in the United States**;
    - public release in any form after approval of the cognizant U.S. Government agency; or
    - *fundamental research* in the U.S. (*See Key Issues in University Research*, Section III.C. *Fundamental Research*, below.)

[32] 22 C.F.R. § 120.15; 15 C.F.R § 734.2(b).

[33] 22 C.F.R. §§ 120.10(a)(5) and 120.11.

- **EAR provision:** The EAR does not control publicly available technology if it is already published or will be published.[34] 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 patents applications available at any patent office; or

    - release at an open conference, meeting, seminar, trade show, or other gathering open to the public.

The EAR requires that the publication is available for distribution free or at price not to exceed the cost of reproduction and distribution; however, the ITAR does not have such a requirement.

Note also that the EAR does not specify where an open conference, meeting, seminar or trade show must take place, and thus allows, for example, participation at a foreign conference so long as the conference is open to all technically qualified members of the public, and attendees are permitted to take notes. Unlike the EAR, the ITAR limits participation in conferences and similar events to those that are taking place in the United States.

B. 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.

- **ITAR provision:** The ITAR specifically provides that the definition of "technical data" does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities.[35]

- **EAR provision:** The EAR provides that publicly available "educational information" is not subject to the EAR, if it is released by instruction in catalogue courses and associated teaching laboratories of academic institutions.[36]

For example, a university graduate course on design and manufacture of very high-speed integrated circuitry will not be subject to export controls, even though the technology is on the CCL. **The key factor is the fact that the information is provided by instruction in a catalogue course**. Foreign students from any country may attend this course because the information is not controlled.

The information will not be controlled even if the course contains recent and unpublished results from laboratory research, so long as the university has not accepted a publication or dissemination restriction.[37]

---

[34] 15 C.F.R. §§ 734.3(b)(3) and 734.7.

[35] 22 C.F.R. § 120.10(a)(5).

[36] 15 C.F.R. §§ 734.3(b)(3) and 734.9.

C. FUNDAMENTAL RESEARCH

During the Reagan administration, several universities worked with the Federal government to establish national policy for controlling the flow of information produced in federally funded fundamental research at colleges, universities and laboratories resulting in the issuance of the National Security Decision Directive 189 ("NSDD"), National Policy on the Transfer of Scientific, Technical and Engineering Information on September 21, 1985. In a letter dated May 24, 2010, President Barrack Obama's administration reaffirmed NSDD 189. NSDD 189 provided the following definition of *fundamental research* that has guided universities in making licensing decisions relative to fundamental research exclusions provided under both the EAR and ITAR.

> *"Fundamental Research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.*

Research conducted by scientists, engineers, or students at a university normally will be considered fundamental research. University based research is not considered *fundamental research* if the university or its researchers accept (at the request, for example, of an industrial sponsor) any access or dissemination restrictions on the project (e.g., publication restriction or foreign national restriction),pursuant to university policy AD 42 the university generally does not accept foreign national restrictions when not required by the federal government. Scientific and technical information resulting from the research will nonetheless qualify as fundamental research once all such restrictions have expired or have been removed.

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. In order to take advantage of this exemption:

- such information 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); [38]
- it is essential to distinguish the information or product that results from the fundamental research from the conduct that occurs within the context of the fundamental research;
- while fundamental research is not subject to export controls, an export license may be required if during the conduct of the research export controlled technology is to be released to a foreign national. Such export controlled technology may come from the research sponsor, from a research partner institution, or from a previous Penn State research project.[39]

---

[37] 15 C.F.R. § 734, Supp. No. 1, Questions C(1) to C(6).

[38] ITAR § 120.11(a)(8); EAR §§ 734.3(b)(3) and 734.8(a).

[39] *See* BIS Revisions and Clarification of Deemed Export Related Regulatory Requirements, 71 Fed. Reg. 30840, 30844 (May 31, 2006). (This interpretation of fundamental research by BIS, while not binding, is instructive as to how DDTC might interpret its regulations.)

One major difference is that the ITAR requires that, to qualify as fundamental research, research must be performed at *accredited institutions of higher learning in the United States*. Under the EAR, fundamental research may occur at facilities other than *accredited institutions of higher learning in the United States*. Information found in EAR 734.8

http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ba2d5996d28cc22033ea2bfb857555cc&rgn=div5&view=text&node=15:2.1.3.4.22&idno=15#15:2.1.3.4.22.0.1.8

Under both the ITAR and the EAR, **research performed at universities will not qualify as fundamental if the university (or the primary investigator) has accepted publication or other dissemination restrictions.**

- **ITAR provision:** the fundamental research exception does not apply to research, the results of which are restricted for proprietary reasons, or specific U.S. Government access and dissemination controls.[40]

- **EAR provision:** the 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.[41] Under the EAR, 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.[42]

The EAR instructs that prepublication review by a sponsor of university research solely to ensure that the publication would not inadvertently divulge proprietary information that the sponsor has initially furnished, or compromise patent rights, does not constitute restriction on publication for proprietary reasons.

The EAR also has provided examples of "specific national security controls" which will trigger export controls. These include requirements for prepublication review and approval by the Government, with right to withhold permission for publication; restriction 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.[43]

While the ITAR does not contain such descriptive provisions, the EAR is instructive as to interpreting the limitations on fundamental research.

[40] 22 C.F.R. §§ 120.11(a)(8) and 120.10(a)(5).

[41] EAR § 734.8(a).

[42] EAR § 734.8(b)(5). However, once the sponsor has reviewed and approved the release, the results may be published as fundamental research.

[43] EAR § 734.11(b).

D. 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 exemption is available only if:

- 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 DDTC; and
- the university documents the disclosure of technical data under the exemption providing: (1) a description of the technical data; (2) the name of the recipient / end-user; (3) the date and time of export; (4) the method of transmission (*e.g.*, e-mail, fax, FedEx); (5) the ITAR reference, *i.e.*, ITAR § 125.4(b)(10), *Full-Time University Employee*.

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*. No exemption is available where the foreign full-time employee will be provided with a *defense service*. A DSP-5 license is required whenever the foreign employee is provided with training in order for the foreign employee to perform his or her job. The key determination here is whether the foreign employee has the technical skill to perform his job, or whether he or she will obtain on-the-job technical training regarding ITAR controlled items or technology. Additionally, if the foreign full-time employee will have technical exchanges with other parties (*e.g.*, the sponsor), then a Technical Assistance Agreement will be required.

THE PENNSYLVANIA STATE UNIVERSITY EXPORT CONTROL PROCEDURES

I. COMMITMENT TO EXPORT CONTROL COMPLIANCE

Penn State conducts focused research to advance knowledge, enhance student learning experiences, and build its reputation in the scientific and technical communities while providing positive returns on sponsoring partners' investments. While Penn State endorses the principles of freedom of inquiry and open exchange of knowledge, it is the university's goal to comply with export controls.

The export of certain technologies, software and hardware is regulated and controlled by Federal law for reasons of national security, foreign policy, prevention of the spread of weapons of mass destruction and for competitive trade reasons. Penn State and all its employees are required to comply with the laws and implementing regulations issued by the Department of State, through its International Traffic in Arms Regulations ("ITAR"), the Department of Commerce, through its Export Administration Regulations ("EAR") and the Department of the Treasury through its Office of Foreign Asset Controls ("OFAC").

In the aftermath of September 11, 2001, and the increased security needs of the United States, the importance and scrutiny of compliance with these regulations has increased, and research contracts and agreements received by universities from sponsors, both Federal and industrial, in which export control provisions are contained, have increased significantly. Export controls regulations apply regardless of the source of funding, both external and internal.

While most research conducted on U.S. college and university campuses is excluded from these regulations under the Fundamental Research Exclusion, university research involving specified technologies controlled under the EAR and/or ITAR, or transactions and exchanges with designated countries, individuals and entities may require Penn State to obtain prior approval from the appropriate agency before allowing foreign nationals to participate in controlled research, collaborating with a foreign company and/or sharing research—verbally or in writing—with persons who are not United States citizens or permanent residents. The consequences of violating these regulations can be quite severe, ranging from loss of research contracts and exporting privileges to monetary penalties and jail time for the individual violating these regulations.

The export control regulations affect not only research conducted on campus, but also travel and shipping items outside the U.S. Simply traveling to certain sanctioned countries could require a license from OFAC. OFAC sanctions prohibit transactions and exchange of goods and services in certain countries and with designated persons and entities. Multiple lists of denied individuals and parties are maintained and enforced by federal agencies including the Departments of State, Commerce, and Treasury. Shipping items outside the U.S. as well as taking controlled items on a flight, even if shipping or traveling in the conduct of research, could require a license from these agencies.

Penn State is committed to export controls compliance, and the export controls compliance unit of the Office of Sponsored Programs ("OSP") is staffed to advise and assist faculty in conducting activities related to research and sponsored programs. More information and resources regarding these and other regulations that impact university activities can be found at http://www.research.psu.edu/osp/manage-awards/export-control, or by contacting the Chair of Export Control Compliance Committee in the Office of Sponsored Programs ("CEC:OSP"), at 814 867-2379.

II. KEY ACTORS RESPONSIBLE FOR EXPORT CONTROL COMPLIANCE

A. EMPOWERED OFFICIAL

The Empowered Official for export control matters at Penn State is the Senior Vice President for Finance and Business. In this capacity, the Empowered Official has the authority to represent the university before the export control regulators in matters related to registration, licensing, commodity jurisdiction requests, or voluntary disclosures. While certain oversight functions may be delegated, only the Empowered Official has the power to sign such paperwork and bind the university in any proceeding before DDTC, BIS, OFAC, or any other government agency with export control responsibilities.

B. CHAIR OF EXPORT CONTROL COMPLIANCE COMMITTEE

The CEC:OSP reports to the Associate Vice President & Director of the Office of Technology Management, and the Director in Office of Sponsored Programs. The CEC:OSP has the authority and the responsibility for the implementation of the procedures set forth in this Export Compliance Program.

The CEC:OSP works closely with the DOSP and the OSP in performing his or her responsibilities. The CEC:OSP:

1. identifies areas at Penn State relative to research that are impacted by export control regulations;
2. develops control procedures to ensure the university remains in compliance;
3. recommends procedures to the OSP Export Control Compliance Committee to strengthen Penn State's compliance with sponsored projects;
4. educates Principal Investigators ("PI"), centers and academic units, graduate students and staff employees about export control regulations and procedures followed at Penn State through outreach and training sessions;
5. monitors and interprets legislation with OSP Export Control Compliance Committee;
6. administers Security Meetings to facilitate understanding and compliance with export controls when creating a Technology Control Plan ("TCP");
7. coordinates Post-award compliance;
8. assists PIs, researchers and offices within Penn State when research or research results are export controlled;
9. seeks legal assistance when uncertain about classification and in filing license applications; and
10. along with the OSP Export Control Compliance Committee, develops a TCP for each export-controlled project consistent with these procedures to aid the PI in meeting his or her export control responsibilities.

C. OFFICE OF SPONSORED PROGRAMS EXPORT CONTROL COMPLIANCE COMMITTEE

The OSP provides assistance and expertise with export controls by working closely with the CEC:OSP and the OSP Export Control Compliance Committee in identifying export control issues and providing support for their solution. The OSP Export Compliance Committee is made up of the following individuals: The CEC:OSP and Negotiators assigned to review export control issues. The OSP Export Control Compliance Committee:

1. provides assistance to OSP negotiators in reviewing the terms of a sponsorship agreement or grant to identify restrictions on publication and dissemination of the research results, and to help OSP negotiators remove such restrictions;

2. provides assistance to the principal investigator as they complete the Export Control Checklist for their project and then discusses with a member of the OSP Export Compliance Committee if export control issues are flagged;

3. is responsible for logging and documenting in SIMS an export review relating to the export concerns of that project;

4. coordinates with the PI's and the CEC:OSP to ensure that foreign nationals will be isolated from participation in an export-controlled project in accordance with the TCP, unless the university applies for and obtains a license from the relevant agency.

The CEC:OSP will conduct training for the university's research community and coordinate the maintenance of an export controls website.

D. KEY UNIVERSITY MANAGERS

Deans, directors, and department heads share the responsibility of overseeing export control compliance in their respective schools or departments, and supporting the OSP Export Control Compliance Committee and OSP in implementing the export compliance program.

E. PRINCIPAL INVESTIGATOR ("PI")

PIs have expert knowledge of the type of information and technology involved in a research project or other university activity. It is the PI's responsibility to 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:

1. must understand his or her obligations under export controls, and participate in all required training to help him or her identify export control issues;

2. each PI must classify the technology involved in the research or other university activity;

3. identify foreign nationals who may be involved and, if export control is likely, initiate the process of clearing foreign national participation with the CEC:OSP, well in advance, to ensure that a license is obtained in a timely manner, or implement proper measures to isolate foreign nationals from participation;

4. must, if undertaking an export controlled project, brief all project personnel (including any graduate or undergraduate students involved in the project) of their obligations related to export controls; and

5. cooperate with the OSP Export Control Compliance Committee in developing the TCP of which the PI has the responsibility to follow and implement. The TCP template is available in Appendix D.

III. EXPORT CONTROL REVIEW

An export control review should be performed when a PI submits a proposal that has a foreign sponsor or foreign sub-agreement, or receives an award with terms and conditions specifically identifying the project as subject to ITAR or EAR, or receives an award that invalidates the Fundamental Research Exemption; e.g., foreign national restriction or publication restriction.

A. INITIAL ASSESSMENT

The OSP Negotiator will look for the following red flags indicating possible export control issues:

1. references to U.S. export regulations (beyond a mere statement of adherence to export control requirements).

2. restrictions on publication or dissemination of the research results;

3. pre-publication approval from sponsor;

4. proprietary or trade secret claims on project results;

5. restriction of access by foreign nationals or participation by U.S. citizens only;

6. involvement of foreign sponsors, collaborators or subrecipients;

7. foreign travel, shipping abroad, or work performed outside the U.S.;

B. EXPORT REVIEW

If the initial assessment flags a possible export control issue, the project will be referred to the OSP Export Control Compliance Committee for further review. The OSP Export Control Committee will have the PI complete the Export Control Checklist in Appendix B, if necessary. Upon completing the review, the OSP Export Control Compliance Committee will advise the PI concerning any export controls which apply to the project, the restrictions on access by foreign persons and/or publication restriction, and any other relevant requirements pursuant to ITAR and EAR.

IV. SECURITY MEETING

The Compliance Coordinator in OSP will schedule a security meeting to discuss the information provided by the PI on the Export Control Review Checklist as well as the project specific security information contained in the award paperwork. The Compliance Coordinator will email Penn State's "What to Expect at a Security Meeting" informational letter to the PI to review and help prepare for the security meeting. The letter can be found in Appendix C.

V. TECHNOLOGY CONTROL PLAN

A. DEVELOPMENT

If the CEC:OSP or the OSP Export Control Compliance Committee determines that a project is export controlled, the Committee will work with the PI to develop and implement a TCP to secure the controlled technology from access by unauthorized foreign persons. The TCP may include:

1. A commitment to export controls compliance
2. Identification of the relevant export control categories and controlled technologies
3. Identification of the project's sponsors
4. General Security Provisions—identification of each individual participating in the project and location of where research will be performed
5. Computer Security Provisions
6. Compliance Provisions
7. Appropriate security measures to be implemented during the project and following project termination
8. Return to Sponsor or Destruction of technology or data

B. APPROPRIATE 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 may 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.
- Personnel Identification. Individuals participating in the project may be required to wear a badge, special card, or other similar device indicating their access to designated project areas. Physical movement into and out of a designated project area may be logged. (*This is not an option that Penn State has used for non-classified research in the past, however, Penn State reserves the right to implement such a requirement if warranted by the specific project*).
- Locked Storage. Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key-controlled access. Hardcopy 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, 128-bit Secure Sockets Layer (SSL) encryption or other federally approved encryption technology. Database access should be managed via a Virtual Private Network (VPN).

- 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 parties must occur only under signed agreements which fully respect the non-U.S. citizen limitations for such disclosures.

C. 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 their College.

VI. LICENSING

If a project is export controlled and a license is needed to involve a foreign national, the Empowered Official may apply for an export license to allow the disclosure of information to foreign students and researchers. Note that each foreign student's participation in each controlled project must be reported to the cognizant licensing agency, even if that student's participation is exempt from licensing requirements. Also note that a TCP, as described in Section V above, must be implemented. Penn State's General Counsel will prepare the documentation for obtaining a license. Penn State's Empowered Official will sign license request.

VII. LICENSE EXCEPTIONS AND EXEMPTIONS RELATED TO TRAVEL OUTSIDE THE U.S.

Travel or transmissions to destinations outside the U.S. can also implicate export control regulations. A license may be required depending on which items are taken, which countries are visited, or whether defense services are provided to a foreign person. However, an exception or exemption from license requirements may exist.

A *License Exception*[44] may be available for EAR controlled items, technology, or software if the individual traveling outside the U.S. can certify that he or she:

1. will ship or hand-carry the items, technology, or software for Penn State business only;
2. will return or certify the destruction of the items, technology, or software within 12 months of leaving the U.S.;
3. will keep the items, technology, or software within his or her effective control;
4. will take necessary security precautions to protect against the unauthorized export of the technology; and
5. will not ship or hand-carry the items, technology, or software to abroad without first consulting with the CEC:OSP.

[44] *See* 15 C.F.R. § 740.1.

A *License Exemption*[45] may be available to ITAR controlled technical data transmitted outside the U.S. if the individual transmitting the technical data can certify that:

1. the technical data is to be used overseas solely by a U.S. person(s);
2. the U.S. person overseas is an employee of Penn State or the U.S. Government and is not an employee of a foreign subsidiary;
3. if the information is Classified*, it will be sent overseas in accordance with the requirements of the Department of Defense Industrial Security Manual; and,
4. no export will be made to countries listed in 22 C.F.R. § 126.1.[46]

Please note that other exceptions or exemptions may be available.

*Penn State does not perform Classified research outside of The Applied Research Laboratory (ARL).

Any individual intending to travel or transmit controlled data outside the U.S. should first consult with the CEC:OSP. All exceptions or exemptions must be documented with the OSP and the record maintained for at least three years after the termination of the project. The certification forms are found in Appendix E. You may also access this information on the Bureau of Industry and Security (BIS) at: http://www.bis.doc.gov/encryption/lechart1_sec508.htm

VIII. TRAINING PROGRAMS

Training is the foundation of a successful export compliance program. Well-informed employees minimize the likelihood that inadvertent violations of the law will occur. The greatest risk of non-compliance of export laws and regulations occurs during casual conversations in person, on the telephone, or via e-mail. The way to prevent these types of violations is through awareness and training.

The CEC:OSP will prepare updated training materials. The CEC:OSP will ensure that every employee or student engaged in an export controlled project receives the appropriate briefing. The CEC:OSP will also maintain records of training provided to employees.

IX. RECORDKEEPING

Penn State's policy is to maintain export-related records on a project basis. Unless otherwise provided for, all records indicated herein shall be maintained consistent with Penn State's record retention policy, and shall be retained no less than three years after the project's TCP termination date or license termination date, whichever is later. Penn State's "General Retention Schedule" and "University Archives Records Management" policy can be found at:

Record Retention Schedule: https://guru.psu.edu/gfug/appendices/APP18.html;

AD35: https://guru.psu.edu/policies/AD35.html

[45] *See* 22 C.F.R. § 125.4.

[46] The full list of proscribed countries may be found at http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf.

If ITAR-controlled technical data is exported under an exemption, certain records of the transaction must be kept five years, which is beyond Penn State's three year retention period.[47] Those records include:

1. a description of the unclassified technical data;
2. the name of the recipient /end-user;
3. the date / time of export;
4. the method of transmission (*e.g.*, e-mail, fax, telephone, FedEx); and
5. the exemption under which the export took place.

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

BIS has specific record-keeping requirements.[48] Generally, records required to be kept by EAR must be kept for a period of five years from the project's termination date. However, if BIS or any other government agency makes a request for such records following a voluntary self-disclosure, the records must be maintained until the agency concerned provides written authorization otherwise.

X. MONITORING AND AUDITING

In order to maintain Penn State's export compliance program and ensure consistent adherence to U.S. export laws, the CEC:OSP may conduct internal reviews of TCPs and certain projects. The purpose of the reviews is: (i) to identify possible violations; and (ii) to identify deficiencies in training, procedures, *etc*., that can be rectified.

XI. DETECTING AND REPORTING VIOLATIONS

It is the policy of Penn State to voluntarily self-disclose violations as required. Since September 11, 2001, government agencies have dramatically increased the investigation in and successful prosecution of export regulation violations. The penalties for these violations can be very severe, including personal liability, monetary fines, and imprisonment. However, government agencies assign great weight to voluntary self-disclosures as a mitigating factor.

Any individual who suspects a violation has occurred must immediately notify the Empowered Official and only the Empowered Official. The Empowered Official will then send an initial notification about the suspected violation to the appropriate government agency.[49] The Empowered Official will conduct an internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. Once the review is complete, the Empowered Official will provide the government agency with a supplementary letter with a thorough narrative account of:

1. the project's description and background

[47] *See* 22 C.F.R. §§ 122.5 and 123.26.

[48] *See* 15 C.F.R. § 762.6.

[49] For EAR violations, see 15 C.F.R. § 764.5. For ITAR violations, see 22 C.F.R. § 127.12(c).

2. a description of the suspected violation
3. which items and controlled categories were involved
4. which dates the violations occurred on
5. which countries were involved
6. who was involved and their citizenships
7. an explanation of why the violation occurred, and
8. any corrective actions taken, and
9. Penn State's commitment to export controls compliance

Once the initial notification and supplementary letter have been sent, the Empowered Official will follow the government agency's instructions.

XII. DISCIPLINARY ACTIONS

In recognition of the seriousness of non-compliance with export controls, Penn State will address non-compliance in accordance with The Pennsylvania State University's policies of RA10, RAG11, RA18, AD65. Further, all Penn State employees responsible for export controls compliance or participating in export-controlled projects must be aware of the substantial criminal and civil penalties imposed for violation of the export regulations including personal liability, monetary fines and imprisonment.

XIII. EMPLOYEE PROTECTION

In accordance with the University's Employee Staff Handbook, 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 Penn State employee will be subject to disciplinary action if the employee knowingly fabricated, knowingly distorted, or knowingly exaggerated the report. The Employee Staff Handbook can be found at:

http://ohr.psu.edu/current-employee/staffhandbook.pdf/atdownload/file

FOREIGN TRAVEL INFORMATION APPENDIX A

Please be aware of the following when traveling abroad and forward to any other personnel who may be traveling for this project.

1. You should be aware that hardware, software, and various materials, chemicals, microorganisms, and toxins taken with you abroad could constitute an export. Technology should be checked against the Munitions List: (http://www.fas.org/spp/starwars/offdocs/itar/p121.htm) and the Commerce Control List (http://www.access.gpo.gov/bis/ear/ear_data.html (Part 774).

2. Most laptops and GPS devices (excluding software or technology that contains source code for 64-bit encryption software or mass market encryption products), and cell phones, are considered "tools of the trade" and are frequently carried abroad, but the investigator carrying these devices abroad must keep it on his or her person **at all times** and make sure the devices are brought back with you. If you plan to leave GPS devices, laptops or mass market encryption products in a foreign country, please inform OSP before you travel. A license from the State Department could be needed before you travel. Software and proprietary data may also be controlled. For more information regarding "tools of the trade", please refer to the Penn State Export Compliance Manual, pages 47 – 53. http://www.research.psu.edu/osp/manage-awards/export-control

3. If project personnel will be providing training to foreign persons (non-students) in the use of ITAR-controlled technology, please inform OSP, because such training could be considered a "defense service."

4. Presentations at international conferences are generally acceptable. It is important to note, however, that sidebar conversations with conference attendees should be limited to information already in the public domain. If the research being discussed in sidebar conversations isn't related in any way to any technologies on the Munitions List or the Commerce Control List, then there's no risk of an export of technical data taking place via a sidebar conversation, regardless of where that conversation takes place. But if your research is related to a listed technology, then you can NOT talk to foreign colleagues about your work unless the conversation is licensed or otherwise exempt. Should you have any questions, please contact OSP for further review.

5. Please note that Penn State's policies on export control can be found here: http://guru.psu.edu/policies/RA18.html and here:
   a. http://guru.psu.edu/policies/RAG11.html (See specifically "PRESENTATION OF PREVIOUSLY UNPUBLISHED RESEARCH DATA AT CONFERENCES").

6. Current travel warnings can be found here: http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html. Register your trip outside the United States with the U.S. Department of State at https://travelregistration.state.gov/ibrs/ui/ Registration allows you to record information about your trip so that the Department of State can assist you in case of an emergency. The FBI advises you to make photo copies of your passport and plane tickets and to keep the copies in separate storage. FBI information for traveling overseas with mobile phones, laptops, PDA's and other electronic devices can be found here: http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure

7. All researchers are encouraged to review the following link: http://www.research.psu.edu/osp/manage-awards/export-control/export-control-fundamentals

8. Please let us know if any additional foreign collaborators are added so a denied party screening can be completed. It is important that you include the name of the organization they are associated with.

Feel free to contact me if you have questions. Thanks!

EXPORT CONTROL APPENDIX B
Review and Documentation Checklist

This review and documentation is required in accordance with University Policy *RA18 Compliance with Federal Export Regulations* and Guideline *RAG11 Guidelines for Ensuring Compliance with Export Control Policy RA18*. Resources and additional information can be found in Section D.

SECTION A – ACKNOWLEDGEMENT

Principal Investigator _____

Sponsor _____

Project Title _____

Agreement No. _____

OSP/Export Log Nos. _____

By signing below, I certify that:

1. I have read and understood this document and have completed the appropriate sections to the best of my knowledge and belief.
2. I understand that I may be held personally responsible for any penalties and fines – **including criminal fines and imprisonment** – that result from failing to comply with or attempting to evade export control law.
3. If the answers to any of the questions in Sections B or C of this checklist should change during the course of the project, I will complete this form again and return the updated form to the Export Control Contact identified below.
4. I will promptly report to the Office of Sponsored Programs any non-compliance or attempt to evade – whether or not through my own personal involvement.
5. My questions regarding these provisions, if any, have been answered.

_____ _____

Principal Investigator Signature Date

Export Control Contact for this project:

Name _____

Phone _____

e-mail _____

SECTION B – FUNDAMENTAL RESEARCH APPLICABILITY

Please answer the following questions in order to determine whether the intended or current research qualifies as Fundamental Research as defined by International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). Definitions and additional information can be found in Section D.

OFFICE OF SPONSORED PROGRAMS PRE-REVIEW

1. Are there any contractual restrictions on the participation of Foreign Nationals/Persons/Organizations on the project? **Yes** ____ **No** ____

2. Will the research results be contractually restricted for proprietary reasons?

This means the University's research results, not any proprietary information provided by Sponsor. **Yes** ____ **No** ____

3. Does the award include any publication restrictions on the scientific and technical information resulting from the project? **Yes** ____ **No** ____

Review-and-comment language <u>does</u> <u>not</u> constitute a publication restriction. Example: allowing 90 days (or less) for a Sponsor to review a proposed publication or presentation for proprietary information provided by Sponsor and to assess the patentability of any invention.

Review-and-approval language <u>does</u> constitute a publication restriction. Example: DFAR 252.204-7000.

Use this space to identify the relevant contract provisions.

PRINCIPAL INVESTIGATOR REVIEW

4. Are you aware of any circumstances that would change the answers to Question 1, 2, or 3, above?

Note: Such circumstances might include informal agreements, Memoranda of Understanding, non-disclosure agreements, Material Transfer Agreements, or other agreements not negotiated by the Office of Sponsored Programs. **Yes** ____ **No** ____

If "Yes," use this space to describe the relevant circumstance(s), agreement(s), etc.

5. Is the research considered to be basic or applied research in science and engineering? **Yes** ____ **No** ____

6. Is all of the research being conducted at accredited institutions of higher learning <u>in</u> the U.S.?

Note: Answer "No" if any research is being conducted at a foreign campus of a domestic institution. **Yes** ____ **No** ____

7. Will the resulting information be published and shared widely ____ ____

PRINCIPAL INVESTIGATOR REVIEW

within the scientific community? ____ ____

To claim the Fundamental Research Exclusion the answers to Questions 1, 2, 3, and 4 must all be "No" and the answers to Questions 5, 6, and 7 must all be "Yes."

8. Based on the answers to Questions 1 through 7 in Section B, can you claim the Fundamental Research Exclusion? **Yes** ____ **No** ____

Proceed to Section C – Export Evaluation.

SECTION C – EXPORT EVALUATION

Please answer the questions in all four sections – Deemed Exports, Physical Exports, Foreign Travel, and Training of Foreign Personnel. Definitions and additional resources and information can be found in Section D.

DEEMED EXPORTS

1. Enter your answer to Section B Question 8 here:
   Can you claim the Fundamental Research Exemption? **Yes** ____ **No** ____
   If "Yes," proceed to PHYSICAL EXPORTS Section.
   If "No," complete Question 2.

2. **Is there any possibility of verbal or written exchange of data/reports with Foreign Nationals/Persons/Organizations?** **Yes** ____ **No** ____

   In addition to students, faculty, or staff participating on this project, this could include Foreign Nationals/Persons/Organizations sharing lab space where the project is being conducted, overhearing project meetings, entering lab space after hours, etc.

   If "No," proceed to PHYSICAL EXPORTS Section.
   If "Yes," complete Question 3.

3. a. I have personally reviewed the U.S. Munitions List and Commerce Control List. (initial here) _____
      See SECTION D — RESOURCES for URLs of lists.

   b. Does the research and/or training performed in the U.S. relate to any technologies on the U.S. Munitions List and/or Commerce Control List? **Yes** ____ **No** ____

   If "No," proceed to PHYSICAL EXPORTS Section.
   If "Yes," complete Questions 4, 5, and 6.

4. **Use this space to identify the specific technologies (including the categories under which they fall on the above lists).**

5. **Use this space to identify the name(s), citizenship(s), and appointment status of all Foreign Nationals/Persons/Organizations who will have access to the laboratories where this work will take place.**

DEEMED EXPORTS

6. It may be necessary to restrict individuals of certain nationalities from accessing your research. Use this space to explain how you propose to segregate the work in your laboratories so that unauthorized Foreign Nationals/Persons/Organizations do not have access to the information generated during the project (including discussions, notebooks, experiments, etc.).

Proceed to Physical Exports Section.

PHYSICAL EXPORTS

1. **Does the intended or current research require the delivery of equipment, technical data, software, materials, or biologicals to a Foreign National/Person?** **Yes** ____ **No** ____

   If "No," proceed to FOREIGN TRAVEL Section.
   If "Yes," complete Questions 2, 3, and 4.

2. **If purchasing the equipment, software, materials, and/or biologicals from a third party, use this space to identify the intended source and, if foreign, the nationality of the foreign source.**
   Example: Items purchased while abroad.

3. **Use this space to identify the name and citizenship of the Foreign Nationals/Persons/Organizations accepting delivery.**

4. a. I have personally reviewed the U.S. Munitions List and Commerce Control List. (initial here) _____ (*10 CFR 810 Assistance to Foreign Atomic Energy Activities*-on a case by case basis consider inserting this language for a nuclear contract)
   See SECTION D — RESOURCES for URLs of lists.

   b. Is/are the equipment, software, materials, and/or biologicals listed on the U.S. Munitions List and/or Commerce Control List? **Yes** ____ **No** ____

   If "No," proceed to FOREIGN TRAVEL Section.
   If "Yes," complete Question 5.

5. Use this space to identify what is being delivered and the specific technologies (including the categories under which they fall on the above lists)

Proceed to Foreign Travel Section.

FOREIGN TRAVEL

1. **Does the intended or current research involve travel to a foreign country?** **Yes** ____ **No** ____

   If "No," proceed to TRAINING OF FOREIGN PERSONNEL Section.
   If "Yes," complete Questions 2, 3, 4, 5 and 6.

FOREIGN TRAVEL

2. Use this space to identify the destination countries.

3. Use this space to provide the name and citizenship of Foreign Nationals/Persons/Organizations with whom you will have contact.

4. Please identify any equipment, materials, software, or technical data that you will be bringing with you or shipping abroad.

5. a. I have personally reviewed the U.S. Munitions List and Commerce Control List. (initial here) _____
See SECTION D — RESOURCES for URLs of lists.

b. Does the research and/or training performed abroad relate to any technologies on the U.S. Munitions List and/or Commerce Control List? **Yes** ____ **No** ____

If "No," proceed to TRAINING OF FOREIGN PERSONNEL Section.
If "Yes," complete Questions 5 and 6.

6. Use this space to identify the specific technologies (including the categories under which they fall on the above lists).

7. If presenting a paper or speaking at a conference, please read and initial by hand the following assurance:
I understand that I may present my research findings in open conference proceedings. However, in one-on-one or small group discussions with conference participants outside open proceedings, I am responsible for complying with any applicable export regulations which may limit discussion to information already in the public domain. (initial here) _____

Proceed to TRAINING OF FOREIGN PERSONNEL Section.

TRAINING OF FOREIGN PERSONNEL

1. Does the intended or current project involve a Foreign National/Person/ Organization who is not a Penn State faculty or staff member or an on-campus student enrolled in a degree program?
Note: This could include a U.S. Person employed by a foreign organization or a Foreign Person employed by a U.S. organization. **Yes** ____ **No** ____
If "No," you have completed the form.
If "Yes," complete Questions 2 and 3.

2. Please use this space to provide the name and citizenship of Foreign Nationals/Persons/Organizations with whom you will have contact, as well as the nature of their involvement in the project.

TRAINING OF FOREIGN PERSONNEL

3. a. I have personally reviewed the U.S. Munitions List and Commerce Control List. (initial here) _____
See SECTION D — RESOURCES for URLs of lists.

b. Will the training or collaborative research relate to any technologies on the U.S. Munitions List and/or Commerce Control List? **Yes** ____ **No** ____

If "No," the form is complete.
If "Yes," complete Questions 4 and 5.

4. Please use this space to identify the specific technologies (including the categories under which they fall on the above lists).

5. It may be necessary to restrict individuals of certain nationalities from accessing the identified technologies. Use this space to explain how you propose to segregate the work in your laboratories so that unauthorized Foreign Nationals/Persons/Organizations do not have access to the ITAR/EAR-controlled technologies.

End of form.

SECTION D – RESOURCES

Lists

United States Munitions List (22 CFR § 121)
http://www.pmddtc.state.gov/regulations_laws/documents/consolidated_itar/Part_121.pdf

Commerce Control List (15 CFR § 774, Supp. 1): http://www.access.gpo.gov/bis/ear/ear_data.html

(review categories 0 – 9)

Foreign Travel

U.S. Department of State Current Travel Warnings: http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html

Penn State Policies and Guidelines

Policy RA18 Compliance with Federal Export Regulations: http://guru.psu.edu/policies/RA18.html

Guideline RAG11 Guidelines for Ensuring Compliance with Export Control Policy RA18:
http://guru.psu.edu/policies/RAG11.html

OSP Resources

Export Toolbox: http://www.research.psu.edu/osp/toolbox/export.html

Definitions

Fundamental Research: 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. See also 22 CFR 120.11. *Note: Generally speaking, "access controls" are restrictions on foreign nationals having access to project information, and "dissemination controls" are restrictions on sharing and/or publishing information. It is not a restriction to allow 90 days (or less) for a Sponsor to review a proposed publication or presentation for proprietary information provided by Sponsor and/or to assess the patentability of any invention.*

Export: The term "export" as used in the various export control regulations has an expansive meaning. An export includes any release or disclosure, including verbal disclosures or visual inspections, of any technology, software, or technical data to any Foreign National/Person. See also ITAR §120.17.

Person: A natural person as well as a corporation, business association, society, trust, or any other entity, organization or group, including government entities. See also ITAR §120.14.

U.S. Person: A Person who is a lawful permanent resident of the U.S. (a citizen of the U.S. or citizen of a foreign country who has been issued a "green card" by the U.S. government), as well as a Person incorporated or organized to do business in the U.S. See also ITAR §120.15.

Foreign National/Person: a Person who is not a lawful permanent resident of the U.S. (includes a person that has not been issued a "green card" by the U.S. government or who possesses only a student visa), as well as a Person not incorporated or not organized to do business in the U.S. See also ITAR §120.16.

Contacts

Office of Sponsored Programs, 110 Technology Center Building, 814-865-1372

ARL Business Office, 227 Applied Research Laboratory, 814-865-6531
Electro-Optics Center, 222 Northpointe Boulevard, Freeport, PA, 724

APPENDIX C

What to Expect at an OSP Security Meeting

If you have been invited to an OSP Security Meeting, this means that the project is subject to export control restrictions which impact export compliance as well as possibly graduate student theses. This document serves as a guide to the Security Meeting process.

The goals of this Meeting are to:

- review the export compliance restrictions imposed on the project
- address all graduate student implications, i.e., foreign national student restriction or publication restriction and its bearing on thesis integrity
- gather the pertinent information from the project participants to create a TCP

Meeting Attendees: Principal Investigators, Chair of Export Control Compliance Committee (CEC:OSP), Compliance Coordinator in OSP, Research Administrators, Department Leads, OSP Negotiators, IT representative, optional attendees are Post Doc's and graduate students.

The meeting will address the information provided by the PI on the Export Control Review Checklist and the project specific security information that will comprise the TCP to ensure the University is compliant with federal requirements of export control. It is important to understand that the Departments of Defense and Commerce have conducted on-site audits of universities and Penn State must be ready to provide records of due diligence when an audit is conducted.

The following provisions will be discussed:

General Security: The CEC:OSP will ask where the project will take place; faculty office and room number, lab space and room number, student offices and room number. Where will the research materials will be kept (locked file cabinet or desk). Where will the project meetings be held and what types of media will be allowed in the secure space? Will the Principal Investigator be sharing project information with a particular person at the sponsor site?

Computer Security: The CEC:OSP will ask about computer security, network security, and data transmission between project personnel and sponsor.

Graduate Student Provisions: if there is a publication restriction, the issue of graduate student thesis integrity and Graduate School approval will be addressed

Compliance: The TCP will be created after the meeting and will be sent to the Research Administrator to obtain signatures of all project personnel, The Department Head, College Dean, and CEC:OSP. The TCP will be kept on file to serve as the basis for evaluation in the event of an on-site security audit by a government agency.

Below is a list of items that may be discussed at the Security Meeting:

- Breaking out restricted vs. non-restricted tasks on your SOW
- Storage, access and transferring of export controlled materials.
- Taking adequate steps to make sure your lab space is secured

    - ✓ card swipe entry vs. key entry
    - ✓ sharing lab space with another faculty member, segregating activities and time
    - ✓ where will project meetings be held so discussions are not overheard

It is important to understand that as the PI, it is your responsibility to make sure that the provisions of the TCP are adhered. If you perform due diligence with the TCP and its provisions, the University will fully support you and your restricted research project. Conversely, if you do not follow the TCP provisions, violation of federal export control carries penalties of fines and imprisonment.

APPENDIX D

(TECHNOLOGY CONTROL PLAN)
THE PENNSYLVANIA STATE UNIVERSITY
University Park, Pennsylvania
Technology Control Plan (TCP)

Re: Sponsor Name
"Project Title"
Principal Investigator:
(Log Nos.)

ACCEPTANCE OF EXPORT CONTROL RESEARCH SECURITY

The undersigned faculty, staff, and graduate students, as a condition of working on the project related to the document referenced above, hereby acknowledge that they have read and agree to abide by the guidelines established in RAG11 and the following specific security provisions:

General Security Provisions

1. No unauthorized foreign person* shall have access to the research or research materials. The following items and/or conditions will be used in the conduct of the research:

   a) Unauthorized foreign persons will not have access to notes, files, or other written or printed research materials. These materials will be kept in a locked cabinet. (In some cases, we may have some research materials that are controlled and other materials which are not. Such distinctions can be identified here. In the absence of clear guidance from the sponsor, we will treat all data and research materials as controlled.)
   b) Project participants will not leave research materials in their workspace when they are not present, even for a short time.
   c) Research meetings will be held in a room where discussions cannot be overheard by unauthorized foreign persons.
   d) The research will be conducted at _____in room_____, which is secure space where foreign nationals will not be present.

2. No publications or release of information will be made without the prior written approval of the Contracting Officer. (Foreign national restrictions or other prior approval requirements should be identified here.)

3. No media of any type, having the capability to replicate and/or copy restricted data will be permitted in (room #). This includes, but is not limited to the following examples of media:

   - Flash drives (thumb drives) unless encrypted
   - Cell phones with camera capability
   - Cameras
   - Any other device that could be used to transfer data.

4. Research materials and data to be exchanged between the University and__(sponsor name here___)may only be exchanged between the following individuals:

   University: PI name
   Sponsor Name: Sponsor contact for exchanges of controlled material

Computer Security Provisions

1. University Policy AD-20 and Guideline ADG02 will be followed.

2. All computer data related to the project will be stored on password protected computers that are not accessible to unauthorized foreign persons. (In some cases, we may have some data that are controlled and other data which are not. Such distinctions can be identified here. In the absence of clear guidance from the sponsor, we will treat all data and research materials as controlled.)

3. Project computers that are connected to the internet or other unsecured networks must be protected behind appropriately configured security appliances (i.e., firewalls).

4. Project computers will have all relevant security patches applied.

5. Any "data at rest" on laptops or removable media must be encrypted to FIPS 140-2 and in compliance with the following DoD Memorandum dated July 3, 2007 :

http://www.dod.mil/pubs/foi/privacy/policy.html (please choose DoD Policy Memo, July 03, 2007)

Any "data at rest" on desktop computers must be encrypted to FIPS 140-2 unless such computers are located in locked rooms to which unauthorized foreign persons will not have unsupervised access. Controlled data may be stored on servers as long as such servers are located in physically-secure facilities to which unauthorized foreign persons will not have unsupervised access. Note that for multiple-user computers or servers, files containing controlled data should either be encrypted or access limited to only authorized users.

(Transfer of Data should be discussed at each Security Meeting with Dave Gindhart and then incorporated into each TCP.)

6. Data residing on a computer connected to the Internet or in transmission through the Internet (e.g. email) will be encrypted by using password protection to avoid inadvertent disclosure. Standard password protection available in commercial software applications such as Microsoft Office products or WinZip is sufficient.

Closeout and Disposition Provisions

The Principal Investigator must work with the Export Compliance Specialist in OSP to ensure that all provisions of the scope of work and Technology Control Plan (TCP) have been met before the end of the project so that the TCP can be closed out. Just some examples of items that could be included here;
[ ] Electronic files and data, excluding technical data that has been approved for publication by Sponsor name, must be removed from all systems, including experimental equipment. Saved data must be disposed of by wiping.
[ ] Hardcopies of all data (including interim and final reports, project notebooks, deliverables, and project data), excluding technical data that has been approved for publication by Sponsor name, should be shredded. If retention is necessary, all retained documents must be properly marked with the following legend and locked in a secure container:

> WARNING - This contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

Citizenship Verfication Procedure

The Chair of Export Control Compliance Committee in Sponsored Programs will verify the U.S. citizenship/Green Card assignment of each signatory on this TCP through the Integrated Business Information Systems (IBIS) software. The citizenship information is provided via the I-9 form completed by the employee at the beginning of their Penn State employment

Please note: If additional personnel are added to the project at a later date, please have the project director obtain their signature on this or a similar form before they begin working on the project and forward to OSP.

Provisions stated above are subject to periodic physical audit.

Name and Date	Name and Date
Name and Date	Name and Date
Name and Date	Name and Date
Name and Date	Name and Date

The College/Unit agrees to provide and oversee the additional security provisions that are necessitated by the terms of the subject grant/contract.

Name and Date

Chair of Export Control Compliance Committee has verified that all signees are U.S. citizens or green card holders.

Name and Date

APPENDIX E

License Exceptions/Exemptions For Travel Outside the U.S.

Department of Commerce

Export License Exception (TMP) for Temporary Exports/Reexports

This exception (TMP) can be used for travel outside the U.S. when you are taking items or technology that would normally require a license from the State Department of Commerce.

What the exception covers:

The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDA's and digital storage devices). The Department of Commerce's Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or reexport of certain items, technology, or software for professional use as long as the criteria in the **EXPORT LICENSE EXCEPTION (TMP) CERTIFICATION** are met.

What the exception does not cover:

The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products and cannot be used for travel to Cuba, Iran, North Korea, Syria or Sudan.
http://www.bis.doc.gov/encryption/lechart1_sec508.htm
http://www.bis.doc.gov/encryption/lechart1.htm

Record-keeping requirements and procedures:

The regulations require the use of this license exception be documented, and records must be kept for five (5) years. Fill out the exception form prior to travel (keep a copy for your files) and return to Wayne Mowery, Chair of Export Control Compliance Committee in the Office of Sponsored Programs, via e-mail @ wmm12@psu.edu. Contact him at (814) 867-2379 if you have questions regarding the exception and procedures.

Export License Exception (BAG) for Temporary Exports/Reexports

LICENSE EXCEPTION (BAG) CERTIFICATION can be used for travel outside the U.S. when you are taking **PERSONAL** items or technology that would normally require a license from the Department of Commerce (see TMP exception above). If you plan to take your personal laptop rather than a laptop from your department when attending a conference or conducting research abroad, and you are taking controlled technology, software, or other information that would require a license, the BAG license exception is available.
To review the exception details **LICENSE EXCEPTION BAG .**

Record-keeping requirements and procedures:

The regulations require the use of this license exception be documented, and records must be kept for five (5) years. Fill out the exception form prior to travel (keep a copy for your files) and return to Wayne Mowery, Chair of Export Control Compliance Committee in the Office of Sponsored Programs, via e-mail @ wmm12@psu.edu. Contact him at (814) 867-2379 if you have questions.

EXPORT LICENSE EXCEPTION (TMP) CERTIFICATION
for Export Administration Regulations (EAR) controlled Items, Technology, and Software

To: University Export Compliance Officer
From: [*Insert Name of PSU PI or Employee*]
Date: [*Insert Date*]
Re: **Export License Exception for Temporary Exports/Reexports***

The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDAs and digital storage devices). The Department of Commerce's Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or reexport of certain items, technology, or software for professional use as long as the criteria to which you are certifying below are met. The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products. In addition, this exception does not apply to items, technology, data, or software regulated by the Department of State's International Traffic in Arms Regulations (ITAR).

Detailed Description of Items, Technology or Software to which this Certification applies:
[*Insert description here*]

By my signature below, I certify that:

1. I will ship or hand-carry the items, technology, or software to [*insert country(s)traveling to*] as a "tool of the trade" to conduct Penn State business only;

2. **I will return the items, technology, or software to the US on** [*insert return date*] **which is no later than 12 months from the date of leaving the US** unless the items, technology, or software are certified by me to have been consumed or destroyed abroad during this 12 month period;

3. I will keep the items, technology, or software under my "effective control" while abroad (defined as retaining physical possession of item or keeping it secured in a place such as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility);

4. I will take security precautions to protect against unauthorized release of the technology while the technology is being shipped or transmitted and used abroad such as:
    a. use of secure connections when accessing e-mail and other business activities that involve the transmission and use of the technology,
    b. use of password systems on electronic devices that store technology, and
    c. use of personal firewalls on electronic devices that store the technology;

5. **I will not ship or hand-carry the items, technology or software to Iran, Syria, Cuba, North Korea, or Sudan without consulting with Penn State's Export Compliance Officer**. If I am planning to travel to these countries, I will consult Penn State's Chair of Export Control Compliance Committee in the Office of Sponsored Programs

Signed: _____ OSP #: _____
[*Name of PI/Employee*] [*if applicable*]

Keep a signed copy with you when traveling abroad

EXPORT LICENSE EXCEPTION (BAG) CERTIFICATION
for Export Administration Regulations (EAR) controlled Items, Technology, and Software

To: University Export Compliance Officer
From: [*Insert Name of PSU PI or Employee*]
Date: [*Insert Date*]
Re: **Export License Exception for Temporary Exports/Reexports***

The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDAs and digital storage devices). The Department of Commerce's Export Administration Regulations (EAR) makes an exception to licensing requirements for the temporary export or reexport of certain items, technology, or software for personal or professional use as long as the criteria to which you are certifying below are met. The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products. In addition, this exception does not apply to items, technology, data, or software regulated by the Department of State's International Traffic in Arms Regulations (ITAR).

Detailed Description of Items, Technology or Software to which this Certification applies:
[*Insert description here*]

By my signature below, I certify that:

1. I personally own the items, technology, or software I am taking abroad to [*insert country(s) traveling to*]
2. I am not shipping the items as unaccompanied baggage;
3. The items, technology, or software are intended for necessary and appropriate personal use only;
4. The items, technology, or software are not intended for sale or other disposal;
5. I will return the items, technology, or software to the U.S.;
6. I will keep the items, technology, or software under my "effective control" while abroad (defined as retaining physical possession of item or keeping it secured in a place such as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility);
7. I will take security precautions to protect against unauthorized release of the technology while the technology is being shipped or transmitted and used abroad such as:
    a. use of secure connections when accessing e-mail and other business activities that involve the transmission and use of the technology,
    b. use of password systems on electronic devices that store technology, and
    c. use of personal firewalls on electronic devices that store the technology;
8. **I will not ship or hand-carry the items, technology or software to Iran, Syria, Cuba, North Korea, or Sudan without consulting with Penn State's Export Control Officer**. If I am planning to travel to these countries, I will consult with Penn State's Chair of Export Control Compliance Committee in the Office of Sponsored Programs.

Signed: _____ OSP #: _____
[*Name of PI/Employee*] [*if applicable*]

Keep a signed copy with you when traveling abroad

LICENSE EXCEPTION (BAG)

740.14 BAGGAGE (BAG)

BAG - BAGGAGE (BAG)

(a) - Scope. This License Exception authorizes individuals leaving the United States either temporarily (i.e., traveling) or longer-term (i.e., moving) and crew members of exporting or reexporting carriers to take to any destination, as personal baggage, the classes of commodities, software and technology described in this section.

(b) - Eligibility. Individuals leaving the United States may export or reexport any of the following commodities or software for personal use of the individuals or members of their immediate families traveling with them to any destination or series of destinations. Individuals leaving the United States who are U.S. persons, as defined in paragraph (b)(4)(i), may export or reexport technology as a tool of trade under paragraph (b)(4) for their personal use or for the personal use of members of their immediate families who are traveling or moving with them, provided they are also U.S. persons, as defined in paragraph (b)(4)(i), to any destination or series of destinations. Technology exports and reexports authorized under paragraph (b)(4) of this section may be made as actual shipments, transmissions, or releases. Individuals leaving the United States temporarily (i.e., traveling) must bring back items exported and reexported under this License Exception unless they consume the items abroad or are otherwise authorized to dispose of them under the EAR. Crew members may export or reexport only commodities and software described in paragraphs (b)(1) and (b)(2) of this section to any destination.

(1) - Personal effects. Usual and reasonable kinds and quantities for personal use of wearing apparel, articles of personal adornment, toilet articles, medicinal supplies, food, souvenirs, games, and similar personal effects, and their containers.

(2) - Household effects. Usual and reasonable kinds and quantities for personal use of furniture, household effects, household furnishings, and their containers.

(3) - Vehicles. Usual and reasonable kinds and quantities of vehicles, such as passenger cars, station wagons, trucks, trailers, motorcycles, bicycles, tricycles, perambulators, and their containers.

(4) - Tools of trade. Usual and reasonable kinds and quantities of tools, instruments, or equipment and their containers and also technology for use in the trade, occupation, employment, location, or hobby of the traveler or members of the household who are traveling or moving. For special provisions regarding encryption commodities and software subject to EI controls, see paragraph (f) of this section. For a special provision that

specifies restrictions regarding the export or reexport of technology under this paragraph, see paragraph (g).
(c) - Limits on eligibility. The export of any item is limited or prohibited, if the kind or quantity is in excess of the limits described in this section. In addition, the items must be:
(b)(4)(i) - For purposes of this paragraph (b), U.S. person is defined as follows: an individual who is a citizen of the United States, an individual who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(2) or an individual who is a protected individual as defined by 8 U.S.C. 1324b(a)(3).
(1) - Owned by the individuals (or by members of their immediate families) or by crew members of exporting carriers on the dates they depart from the United States;
(2) - Intended for and necessary and appropriate for the use of the individuals or members of their immediate families traveling with them, or by the crew members of exporting carriers;
(3) - Not intended for sale or other disposal; and
(4) - Not exported under a bill of lading as cargo if exported by crew members.
(d) - Special provision: unaccompanied baggage. Individuals departing the United States may ship unaccompanied baggage, which is baggage sent from the United States on a carrier other than that on which an individual departs. Crew members of exporting carriers may not ship unaccompanied baggage. Unaccompanied shipments under this License Exception shall be clearly marked "BAGGAGE." Shipments of unaccompanied baggage may be made at the time of, or within a reasonable time before or after departure of the consignee or owner from the United States. Personal baggage controlled for chemical and biological weapons (CB), missile technology (MT), national security (NS), encryption items (EI) or nuclear nonproliferation (NP) must be shipped within 3 months before or after the month in which the consignee or owner departs the United States. However, commodities controlled for CB, MT, NS, EI or NP may not be exported under this License Exception as unaccompanied baggage to Country Groups D:1, D:2, D:3, D:4, or E:1. (See Supplement No. 1 of this part).
(e) - Special provisions: shotguns and shotgun shells
(1) - A United States citizen or a permanent resident alien leaving the United States may export or reexport shotguns with a barrel length of 18 inches or over and shotgun shells under this License Exception, subject to the following limitations:
(i) - Not more than three shotguns may be taken on any one trip.
(ii) - The shotguns and shotgun shells must be with the person's baggage but they may not be mailed.
(iii) - The shotguns and shotgun shells must be for the person's exclusive use for legitimate hunting or lawful sporting purposes, scientific purposes, or personal protection, and not

for resale or other transfer of ownership or control. Accordingly, except as provided in (e)(2) of this section, shotguns may not be exported permanently under this License Exception. All shotguns and unused shotgun shells must be returned to the United States. Note that since certain countries may require an Import Certificate or a U.S. export license before allowing the import of a shotgun, you should determine the import requirements of your country of destination in advance.
(2) - A nonresident alien leaving the United States may export or reexport under this License Exception only such shotguns and shotgun shells as he or she brought into the United States under the provisions of Department of Justic Regulations (27 CFR 478.115(d)).
(f) - Special provisions: encryption commodities and software subject to EI controls on the Commerce Control List.
(1) - A U.S. citizen or permanent resident alien of the United States as defined by 8 U.S.C. 1101(a)(20) may use this license exception to export or reexport encryption commodities and software to any destination not in Country Group E:1 of Supplement No. 1 of this part.
(2) - A person other than a U.S. citizen or permanent resident alien of the United States as defined by 8 U.S.C. 1101(a)(20) (except a national of a country listed in Country Group E:1 of Supplement No. 1 of this part who is not a U.S. citizen or permanent resident alien of the United States) may also use this license exception to export or reexport encryption commodities and software to any destination not in Country Group E:1 of Supplement No. 1 of this part.
(b)(4)(ii) - [RESERVED]
(g) - Special provision: restrictions for Export or Reexport of Technology. This authorization for the export or reexport of technology under the tools of trade provisions of paragraph (b)(4) of this section may be used only if:
(g)(1) - The technology is to be used overseas solely by individuals or members of their immediate families traveling with them provided they are U.S. persons as defined in paragraph (b)(4)(i).
(g)(2) - The exporting or reexporting party and the recipient take adequate security precautions to protect against unauthorized access to the technology while the technology is being transmitted and used overseas. Examples of security precautions to help prevent unauthorized access include the following:
(g)(2)(i) - Use of secure connections, such as Virtual Private Network connections when accessing IT networks for e-mail and other business activities that involve the transmission and use of the technology authorized under this license exception;
(g)(2)(ii) - Use of password systems on electronic devices that

will store the technology authorized under this license exception; and
(g)(2)(iii) - Use of personal firewalls on electronic devices that will store the technology authorized under this license exception.
(g)(3) - The technology authorized under these provisions may not be used for foreign production purposes or for technical assistance unless authorized by BIS;
(g)(4) - Any encryption item controlled under ECCN 5E002 is not exported or reexported to any destination listed in Country Group E:1 of Supplement No. 1 of this part.

(Compiled by Vanderbilt University)