

Export Controls Compliance
State University of New York
at Stony Brook University

Revised July 2024

The purpose of this document is to provide overall guidance on export control regulations and internal procedures. For additional information or assistance, please contact Susan Gasparo, Director of Research Security, Export Compliance Officer via email at Susan.gasparo@stonybrook.edu or at 631-632-1954, or Terrence Rusch, Research Security Administrator, Export Compliance Officer at terrence.rusch@stonybrook.edu, 631-632-1925.

OVERVIEW.....	4
INSTITUTIONAL COMMITMENT.....	4
WHAT ARE EXPORT CONTROLS?	4
WHAT IS AN EXPORT?.....	5
WHO IS A FOREIGN PERSON?.....	5
WHY DOES EXPORT COMPLIANCE MATTER TO ME?	5
REGULATIONS	6
INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)	6
EXPORT ADMINISTRATION REGULATIONS (EAR)	14
NUCLEAR EXPORT CONTROL REGULATIONS.....	17
FOREIGN ASSETS CONTROL REGULATIONS (FARC)	17
RESTRICTED PARTIES	19
PENALTIES/SANCTIONS	21
RECORD KEEPING	22
RESEARCH AND EDUCATIONAL ACTIVITIES	23
NATIONAL SECURITY DECISION DIRECTIVE 189 (NSDD189)	23
FUNDAMENTAL RESEARCH	23
FUNDAMENTAL RESEARCH EXCLUSION	24
PUBLIC DOMAIN/PUBLICLY AVAILABLE INFORMATION	25
EDUCATIONAL INFORMATION	27
EXEMPTIONS FOR EMPLOYEES.....	27
EXPORT CONTROL COMPLIANCE GUIDANCE.....	28
MYRESEARCH – EXPORT REVIEW QUESTIONS	28
ELECTRONIC COMMUNICATIONS (E-MAIL, FAX, AND SHARE DRIVES)	28
ENCRYPTION	28
FOREIGN PERSONS	29
DEEMED EXPORTS	29
I129 EXPORT ATTESTATION REQUIREMENT	29

VISITORS	30
FOREIGN TRAVEL.....	30
INTERNATIONAL COLLABORATIONS.....	32
MEMORANDUM OF UNDERSTANDING (MOU).....	32
PROPRIETARY INFORMATION	33
PUBLICATION/FOREIGN PERSON RESTRICTIONS	33
RECEIPT OF MATERIALS, EQUIPMENT, TECHNOLOGY AND TECHNICAL INFORMATION/DATA ...	33
SHIPPING: SENDING MATERIALS, EQUIPMENT, TECHNOLOGY, AND TECHNICAL INFORMATION	34
SERVICE CENTERS (IFRS AND S&FS).....	35
TECHNOLOGY CONTROL PLANS	36
INTERNAL EXPORT CONTROL COMPLIANCE ROLES AND RESPONSIBILITIES.....	36
WHO PARTICIPATES IN A COMPLIANCE PROGRAM?	36
ESCALATION PROCESS.....	36
LEGAL COUNSEL.....	36
EXPORT COMPLIANCE PROGRAM	37
CAMPUS OFFICES	38
FACULTY AND STAFF.....	40
EXPORT REVIEW PROCESS, CLASSIFICATIONS, LICENSE EXCEPTIONS AND LICENSES.....	41
EXPORT REVIEW PROCESS.....	41
ITEM/TECHNOLOGY CLASSIFICATION	42
LICENSE EXCEPTIONS.....	44
LICENSES	44
VOLUNTARY DISCLOSURE	45
AUDIT INTERNAL ASSESSMENTS.....	45
TRAINING AND EDUCATION.....	46

OVERVIEW

INSTITUTIONAL COMMITMENT

Stony Brook University (“University or “SBU”) is committed to the highest level of compliance with all applicable export control laws and regulations that pertain to the conduct and dissemination of our research and to the export of tangible items such as equipment, components, or materials. While our primary mission is education, research and dissemination of knowledge, the responsibility remains to balance the services of this mission with safeguarding national assets through adherence of the export regulations, rules, and laws of our country. In the [November 19, 2010 memorandum](#), John J. O’Connor reaffirmed the commitment by the State University of New York (SUNY) and The Research Foundation for State University of New York (RF) to assure due diligence and compliance with the U.S. federal government export control laws and regulations. The purpose of this document is to restate for the SBU campus community the essential aspects of the laws and regulations concerning exports, confirm [our policy](#) for compliance, and explain how SBU will provide our campus community with the assistance they may need to ensure compliance with these complicated laws.

WHAT ARE EXPORT CONTROLS?

Generally stated, export controls regulate the disclosure, shipment, use, transfer or transmission of any item, commodity, material, technical information, technology, or software, and encrypted software appearing on the U.S. government's export-controlled lists for the benefit of a foreign person or foreign entity anywhere. Additionally, export controls regulate transactions or the provision of services including those involving prohibited countries, persons, entities, or conduct based on trade sanctions, embargoes and restrictions on travel or activities by U.S. Persons. These restrictions also extend to foreign persons while they are present in the U.S. The four main bodies of federal export control regulations applicable to the university (and campus community) are the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), the Foreign Assets Control Regulations (FACR), and the Assistance to Foreign Atomic Energy Activities (AFAEA). However, other federal agencies also

regulate the export, re-export or re-transfer of certain items and technologies as well as imports of items and technologies into the U.S.

WHAT IS AN EXPORT?

There are several meanings* of the word “export,” which include any of the following:

- Actual shipment of any covered goods or items; or
- The electronic or digital transmission of any covered goods, items, or related goods or items; or
- Any release or disclosure, including verbal disclosures or visual inspections, or any technology, software or technical data to any foreign person wherever located; or
- Actual use or application of covered technology on behalf of or for the benefit of any foreign entity or person anywhere.

**For the precise definition for each regulation, please see “Regulations.”*

WHO IS A FOREIGN PERSON?

The federal definition of a “foreign person” is a person who is **NOT**:

- Granted permanent U.S. residence, as demonstrated by the issuance of a permanent residence card, i.e., a "Green Card."
- Granted U.S. citizenship.
- Granted status as a "protected person" under 8 U.S.C. 1324 b(a)(3), e.g., political refugees, political asylum holders).

It also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the U.S., as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

WHY DOES EXPORT COMPLIANCE MATTER TO ME?

While most university and research activities do not require an export control license, there are times when an export license or documentation of compliance with the regulations is required.

All members of the Campus Community¹ are required to demonstrate their due diligence and

¹ Campus Community includes but is not limited to all faculty (including voluntary, lecturers, and adjuncts); research

to document their adherence to the applicable laws and regulations. These basic questions should be asked when partaking in activities that require the transfer of information and/or items.

- What type of activity are you doing?
- What items or technologies are being used?
- Where are any items or technologies going?
- Who will access the items or technologies?
- Why? For what will the end-user be using the items or technologies?

For most situations on campus*:

- Technology is defined as the “information necessary for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of an item” (EAR §772.1)
- “Technology can be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer aided design files, manuals or documentation, electronic media or information revealed through visual inspection” (EAR §772.1)

**In instances where the project is for military applications or includes equipment or technical information under the International Traffic Regulations (ITAR), definitions from the ITAR prevail.*

REGULATIONS

INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

Authority

22 CFR §§ 120-130 are promulgated and implemented by the Directorate of Defense Trade Controls (“DDTC”) in the Department of State (“DoS”) and regulate defense articles (as defined in §120.31), significant military equipment (as defined in §120.36), major defense equipment

personnel (including research staff, post-doctoral fellows, research associates); visiting scientists and scholars, graduate and undergraduate students involved in research activities; visiting scholars, consultants or other volunteers involved in research activities; non research staff in departments, centers, institutes, colleges, administrative offices that are involved with transactions covered under this policy.

(as defined in §120.37), defense services (as defined in §120.32), and technical data and software (as defined in §120.33).

ITAR Decision Trees

Unavailable - currently being re-designed by Department of State

Quick Facts

- If a United States Military List (USML) article is incorporated into a larger article, then the larger article becomes controlled under ITAR.
- ITAR is article-based: NO article on the USML can be exported without a license or exemption.
- Arms Embargo: NO article on the USML may be exported under a license or license exemption to countries proscribed in 22 CFR § 126.1.
 - o Additional restrictions apply to other countries, whenever an export would not otherwise be in furtherance of world peace and the security and foreign policy of the United States – as proscribed further in 22 CFR § 126.1.

Policy on designating and determining defense articles and services (22 CFR § 120.3)

- a) For purposes of this subchapter, a specific article or service may be designated a defense article (see § 120.31) or defense service (see § 120.32) if it:
- 1) Meets the criteria of a defense article or defense service on the U.S. Munitions List (USML) (part 121 of this subchapter); or
 - 2) Provides the equivalent performance capabilities of a defense article on the USML.
- b) For purposes of this subchapter, a specific article or service shall be determined in the future as a defense article or defense service if it provides a critical military or intelligence advantage such that it warrants control under this subchapter.

Note 1 to paragraphs (a) and (b): An article or service determined in the future pursuant to this subchapter as a defense article or defense service, but not currently on the USML, will be placed in Category XXI of § 121.1 of this subchapter until the appropriate category of the USML has been amended to provide the necessary entry.

- c) A specific article or service is not a defense article or defense service for purposes of this subchapter if it:
- 1) Is determined to be under the jurisdiction of another department or agency of the U.S.

Government (see § 120.5) pursuant to a commodity jurisdiction determination (see § 120.4) unless superseded by changes to the USML or by a subsequent commodity jurisdiction determination; or

- 2) Meets one of the criteria of § 120.41(b) when the article is used in or with a defense article and specially designed is used as a control criteria.

Note 2 to § 120.3: The intended use of the article or service after its export (i.e., for a military or civilian purpose), by itself, is not a factor in determining whether the article or service is subject to the controls of this subchapter.

Note: There are items that were classified as defense articles when created that may now have a research and/or commercial application – however, these items unless deregulated by the government remain subject to the ITAR.

ITAR Definitions

Defense Article (22 CFR § 120.31)

- a) Defense article means any item or technical data designated in § 121.1 of this subchapter and includes:
 - 1) Technical data recorded or stored in any physical form, models, mockups, or other items that reveal technical data directly relating to items designated in § 121.1 of this subchapter; and
 - 2) Forgings, castings, and other unfinished products, such as extrusions and machined bodies, which have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles.
- b) It does not include basic marketing information on function or purpose or general system descriptions.
- c) The policy described in § 120.3 is applicable to designations of additional items.

Significant Military Equipment (22 CFR § 120.36)

- a) Significant military equipment means articles for which special export controls are warranted because of their capacity for substantial military utility or capability.
- b) Significant military equipment includes:
 - (1) Items in § 121.1 of this subchapter that are preceded by an asterisk; and
 - (2) All classified articles enumerated in § 121.1 of this subchapter.

Major Defense Equipment (22 CFR § 120.37)

Major defense equipment, pursuant to section 47(6) of the Arms Export Control Act (22 U.S.C. 2794(6)), means any item of significant military equipment on the U.S. Munitions List having a nonrecurring research and development cost of more than \$50,000,000 or a total production cost of more than \$200,000,000.

Defense Service (22 CFR § 120.32)

- 1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles;
- 2) The furnishing to foreign persons of any technical data controlled under this subchapter, whether in the United States or abroad; or
- 3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

Technical Data (22 CFR § 120.33)

- a) for purposes of this subchapter:
 - 1) Information, other than software as defined in §120.40(g), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation.
 - 2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;
 - 3) Information covered by an invention secrecy order; or
 - 4) Software (see §120.40(g)) directly related to defense articles.
- b) The definition in paragraph (a) of this section does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in §120.34 or telemetry data as defined in note 3 to Category XV(f) of part 121.1 of this subchapter. It also does not include

basic marketing information on function or purpose or general system descriptions of defense articles.

[Export \(22 CFR §120.50\)](#)

- a) Export, except as set forth in § 120.54 or § 126.16 or § 126.17 of this subchapter, means:
- 1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;
 - 2) Releasing or otherwise transferring technical data to a foreign person in the United States (a deemed export);
 - 3) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to this subchapter by a U.S. person to a foreign person;
 - 4) Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;
 - 5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or
 - 6) The release of previously encrypted technical data as described in § 120.56(a)(3) and (4).

Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

[Reexport \(22 CFR §120.51\)](#)

- a) Reexport, except as set forth in §120.54, §126.16 or §126.17, of this subchapter means:
- 1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;
 - 2) Releasing or otherwise transferring technical data to a foreign person who is a citizen or permanent resident of a country other than the foreign country where the release or transfer takes place (a
 - 3) “Deemed reexport”)
 - 4) Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to this subchapter between foreign persons.
- b) Any release outside the U.S. of technical data to a foreign person is deemed to be a reexport

to all countries in which the foreign person has held or holds citizenship or holds permanent residency.

[Release \(22 CFR §120.56\)](#)

(a) Release. Technical data is released through:

- 1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; or
- 2) Oral or written exchanges with foreign persons of technical data in the U.S. or abroad.
- 3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or
- 4) The use of access information to cause technical data outside of the United States to be in unencrypted form.

(b) Provision of access information. Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.

[Access information \(22 CFR §120.55\)](#)

Access information is information that allows access to encrypted technical data subject to this subchapter in an unencrypted form. Examples include decryption keys, network access codes, and passwords.

[Retransfer \(22 CFR §120.52\)](#)

(a) Retransfer, except as set forth in §120.54, §126.16, or §126.17, of this subchapter means:

- 1) A change in end use or end user, or a temporary transfer to a third party, of a defense article within the same foreign country; or
- 2) A release of technical data to a foreign person who is a citizen or permanent resident of the country where the release or transfer takes place.

(b) [Reserved]

[Activities that are not exports, reexports, retransfers, or temporary imports" \(22 CFR §120.54\)](#)

a) The following activities are not exports, reexports, retransfers, or temporary imports:

- 1) Launching a spacecraft, launch vehicle, payload, or other item into space.
- 2) Transmitting or otherwise transferring technical data to a U.S. person in the United States

from a person in the United States.

- 3) Transmitting or otherwise transferring within the same foreign country technical data between or among only U.S. persons, so long as the transmission or transfer does not result in a release to a foreign person or transfer to a person prohibited from receiving the technical data.
- 4) Shipping, moving, or transferring defense articles between or among the United States as defined in §120.60.
- 5) Sending, taking, or storing technical data that is:
 - i. Unclassified;
 - ii. Secured using end-to-end encryption.
 - iii. Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128); and
 - iv. Not intentionally sent to a person in or stored in a country proscribed in §126.1 of this subchapter or the Russian Federation;
Note to paragraph (a)(5)(iv): Data in-transit via the internet is not deemed to be stored.
 - v. Not sent from a country proscribed in §126.1 of this subchapter or the Russian Federation.

b)

- 1) For purposes of this section, end-to-end encryption is defined as:
 - i. The provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and

- ii. The means of decryption are not provided to any third party.
- 2) The originator and the intended recipient may be the same person. The intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, such as by a license or other approval pursuant to this subchapter.
- c) The ability to access technical data in encrypted form that satisfies the criteria set forth in paragraph (a)(5) of this section does not constitute the release or export of such technical data.

United States Munitions List (USML) 22 CFR § 121

Regulated items are identified on the USML in the following categories:

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

- Category XVII-Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
- Category XVIII-Directed Energy Weapons
- Category XIX-Gas Turbine Engines and Associated Equipment
- Category XX-Submersible Vessels and Related Articles
- Category XXI-Articles, Technical Data, and Defense Services Not Otherwise Enumerated

[Where are complete versions of the ITAR and USML available?](#)

https://www.pmdotc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=%2024d528fddbfc930044f9ff621f961987

EXPORT ADMINISTRATION REGULATIONS (EAR)

Authority

CFR Parts 730-774 are promulgated and implemented by the Department of Commerce, Bureau of Industry and Security (BIS), and regulate the export control, the export and re-export of commercial and dual use (commercial and military/security applications) items, including encrypted software, identified on the Commerce Control List (CCL).

EAR Decision Tree

<https://www.bis.doc.gov/index.php/decision-tree-tools>

Quick Facts

- Items not designated under the control of another federal agency or listed on the Commerce Control List (CCL) are classified as EAR99.
- The CCL is destination based and export or re-export of both ECCN designated items and EAR99 items are controlled based upon the country of destination.

EAR Unique Definitions

Access Information (15 CFR § 772.1)

Access information means information that allows access to encrypted technology or encrypted software in an unencrypted form. Examples include decryption keys, network access codes, and passwords.

Export (15 CFR § 734.13)

- 1) an actual shipment or transmission out of the U.S., including the sending or taking of an item out of the U.S., in any manner.,
- 2) releasing or otherwise transferring of “technology” or source code (but not object code) to a foreign person in the U.S. (a “deemed export”) or transferring by a person in the U.S. of registration, control, or ownership of spacecraft ... (see §734.13(a)(3)).

An export of an item that will transit through a country or countries to a destination identified in the EAR is deemed to be an export to that destination.

Re-export (15 CFR § 734.14)

- 1) an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;
- 2) releasing or otherwise transferring “technology” or source code subject to the EAR to a foreign person of a country other than the foreign country where the release or transfer takes place (a deemed re-export); (3) transferring by a person outside of the U.S. of registration, control, or ownership of spacecraft (see 734.14(a)(3)).

Release as used in (15 CFR § 734.15)

- a) Technology or software is “released” through:
 - I. Visual or other inspection by foreign person of items that reveal “technology” or source code subject to the EAR to a foreign person; or
 - II. Oral or written exchanges with a foreign person of “technology” or source code In the U.S. or abroad
- b) Any act causing the “release” of “technology” or “software,” through the use of “access information” or otherwise, to yourself or another person requires an authorization to the same extent an authorization would be required to export or reexport such “technology” or “software” to that person.

NOTE: Export of encryption source code and object code has special rules, see 15 CFR § 734.17

Export Control Classification Number (ECCN)

The alpha-numeric designation proscribed to a particular item on the CCL according to category

and group.

EAR99

If an item falls under U.S. Department of Commerce jurisdiction and is not listed on the CCL, it is designated as EAR99. EAR99 items consist of low-technology consumer goods and do not require a license in many situations. However, if the proposed export of an EAR99 item is to an embargoed country, to an end-user of concern or in support of a prohibited end-use, you may be required to obtain a license.

Commerce Control List (CCL) 15 CFR § 774 Supplement 1

Regulated items are identified on the CCL in the following ten broad categories:

- 0-Nuclear Materials, Facilities and Equipment and Miscellaneous Items
- 1-Materials, Chemicals, "Microorganisms," and Toxins
- 2-Materials Processing
- 3-Electronics Design, Development, and Production
- 4-Computers
- 5 Part 1-Telecommunications
- 5 Part 2-Information Security
- 6-Sensors and Lasers
- 7-Navigation and Avionics
- 8-Marine
- 9-Aerospace and Propulsion

Within each category, items are arranged by group:

- A-Equipment, Assemblies, and Components
- B-Test, Inspection, and Production Equipment
- C-Materials
- D-Software
- E-Technology

Where are complete versions of the EAR and CCL available?

<https://www.bis.gov/ear>

NUCLEAR EXPORT CONTROL REGULATIONS

Authority

- 10 CFR Part 810, the Assistance to Foreign Atomic Energy Activities (AFAEA) is promulgated and implemented by the Department of Energy (DOE) and regulates technology and services related to direct or indirect production of Special Nuclear Materials. Licensing is through the National Nuclear Security Agency (NNSA).
- 10 CFR Part 110 is promulgated and implemented by the Nuclear Regulatory Commission (NRC) and regulates major hardware, components, and nuclear material.

Quick Facts 10 CFR Part 810

- Special Nuclear Materials means plutonium, uranium-233, or uranium enriched above 0.711 percent by weight in the isotope uranium-235.
- Activities are either out of scope (not subject to 10 CFR Part 810), generally authorized, or require specific authorization.

Quick Facts 10 CFR Part 110

- Imports and exports of major and minor reactor equipment. “Nuclear Reactor” is defined as items within or attached directly to the reactor vessel and specially designed or prepared.
- Controls include software.
- General and specific licenses.

Where are complete versions of the AFAEA and NRC regulations available?

http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title10/10cfr810_main_02.tpl

<http://www.nrc.gov/reading-rm/doc-collections/cfr/part110/full-text.html>

FOREIGN ASSETS CONTROL REGULATIONS (FARC)

Authority

- 31 CFR Parts 500-597 are promulgated and implemented by the U.S. Treasury Department, Office of Foreign Assets Control and regulate economic trade with foreign countries. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists,

international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

- The Trading with the Enemy Act (TEWA), 50 U.S.C. §§ 1-44, which gives the President the power to restrict and oversee all trade between the United States and its enemies during the time of war.
- International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706, which allows the President to identify any unusual, extraordinary threat that originates outside the United States and to confiscate property and prohibit transactions in response.
- Specially Designated Nationals and Blocked Persons List, 15 C.F.R. Part 764, Supplement 3, comprised of individuals and organizations deemed to represent restricted countries or known to be involved in terrorism and narcotics trafficking. At present, OFAC administers seventeen sanctions programs, including Cuba, Syria, Iran, and North Korea, and the Specially Designated Nationals and Blocked Persons list.

Note: Sanction programs and the Specially Designated Nationals and Blocked Persons list are subject to change and are updated routinely.

Cuba

Limited travel (as specified by general licenses) is allowed to Cuba. The U.S. government has an embargo against Cuba. Changes to general licenses for travel were updated in late 2020. All travel to Cuba for any university related activity must be reviewed and approved by the Export Compliance Officer prior to travel.

- Department of Treasury, Cuba sanctions: <https://ofac.treasury.gov/sanctions-programs-and-country-information/cuba-sanctions>
- Department of Commerce, Cuba guidance: <https://www.bis.gov/articles/cuba-export-controls>

Iran

Iran is one of the most-heavily sanctioned countries and all activities in Iran require a license from the U.S. Department of Treasury. Any item being sent to or hand-carried to Iran will most likely require a license from the U.S. Department of Commerce. Prior review and approval by the Export Compliance Officer is required before engaging in any activities or traveling to Iran

for any university related purposes.

- Department of Treasury, Iran sanctions: <https://ofac.treasury.gov/sanctions-programs-and-country-information/iran-sanctions>
- Department of Commerce, Iran guidance: <https://www.bis.gov/articles/iran-export-controls>

Where is the complete list of OFAC sanction programs and a complete version of the FARC available?

- OFAC Sanction Programs: <https://ofac.treasury.gov/sanctions-programs-and-country-information>
- FARC: http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title31/31cfrv3_02.tpl

Anti-Boycott Regulations

Anti-Boycott laws are administered and enforced by the Department of Commerce, Bureau of Industry Security, under the “Restrictive Trade Practices and Boycotts” of the EAR (15 CFR Part 760) and by the Department of Treasury under the “Ribicoff Amendment” to the Tax Reform Act of 1976 adding §999 to the Internal Revenue Code. Anti-Boycott regulations prohibit U.S. businesses from taking actions in support of unsanctioned foreign boycotts, including the Arab League’s boycott of Israel. They also prevent U.S. persons from conducting business under terms that would restrict a person’s ability to do business with other countries under a boycott not recognized by the United States.

RESTRICTED PARTIES

WHAT IS A RESTRICTED PARTY?

A restricted party is an entity that is placed on a denial list by the U.S. government or any other country’s government. A license from one, or more, of the federal agencies may be required if you plan to conduct any business or research with a restricted party, even if you are conducting Fundamental Research.

WHO CAN BE A RESTRICTED PARTY?

Anyone! Restricted parties are not limited to foreign persons and entities and can include U.S. persons. Additionally, numerous foreign universities have been designated restricted parties. Restricted parties are subject to change and are updated routinely. Restricted party designation

is not based upon nationality but instead is based upon previous behavior or action.

GOVERNMENT RESTRICTED PARTIES LISTS

There are over fifty lists issued by U.S. governmental agencies that restrict transactions with specific individuals, groups, and entities, which include the following:

Department of Commerce

- **Denied Persons List** is a list of individuals and entities that have been denied export privileges. Any dealings with a party on this list would violate the terms of its denial order and is prohibited.
- **Entity List** is a list of parties whose presence in a transaction can trigger a license requirement under the EAR. The license requirements are in addition to any license requirements imposed on the transaction by other provisions of the EAR.
- **“Unverified” List** is a list of parties where the Bureau of Industry and Security has been unable to verify the end-user in prior transactions.
- **Military End-User List** is a non-exhaustive listing of entities or individuals in foreign countries subject to additional restrictions under the EAR.

Department of State

- **Debarred List** is a list of parties who are barred by 22 CFR §127.7 (ITAR) from participating directly or indirectly in the export of defense articles, including technical data or in the furnishing of defense services for which a license or approval is required by ITAR.
- **Nonproliferation Sanctions** is a list of parties that have been sanctioned under various statutes.

Department of Treasury

- **Specially Designated Nationals and Blocked Persons** is a list of individuals and organizations deemed to represent restricted countries or known to be involved in terrorism and narcotics trafficking.

DESCARTES VISUAL COMPLIANCE

The RF has licensed Descartes Visual Compliance (Descartes), which is a software suite that allows SBU to screen for restricted parties. The SBU Campus Community can access Descartes by registering with their @stonybrook.edu email at <https://www.visualcompliance.com/usr>.

PENALTIES/SANCTIONS

WHO CAN BE PENALIZED?

Penalties can apply to individuals and to the organization! The penalties listed below are 2020 figures, penalties are increased for inflation on an annual basis.

VIOLATIONS OF ITAR

- Criminal Penalties (for willful violation): entity of up to \$1,000,000 for each violation; individuals may be subject to a fine of up to \$1,000,000 or imprisonment of up to ten years, or both, for each violation.
- Civil Penalties: entity up to \$1,163,217 for each violation; individuals may be subject to fines of up to \$1,163,217 for each violation. In addition, suspension, or debarment from government contracts; seizure or forfeiture of the item; and/or revocation of export privileges.

VIOLATIONS OF THE EAR

- Criminal Penalties (for willful violation): may result in the institution paying a fine of up to \$1,000,000 or five times the value of the exports (whichever is greater) for each violation; and the individual may be fined up to \$250,000 or be imprisoned for up to ten years, or both, for each violation.
- Criminal Penalties (for knowing violation): may result in the institution paying a fine of up to the greater of \$50,000 or five times the value of the exports for each violation; and the individual may be fined up to the greater of \$50,000 or five times the value of the exports or be imprisoned for up to five years, or both, for each violation.
- Civil Penalties: include \$12,000 for each violation, except that the fine for violations involving items controlled for national security reasons is up to \$120,000 for each violation; suspension or debarment from government contracts; seizure or forfeiture of the item; and/or revocation of export privileges. Additionally, for each violation, any or all of the following sanctions may be imposed:
 - The denial of export privileges; and/or
 - The exclusion from exporting practice; and/or
 - Loss of federal funds

- Seizure/Forfeiture of goods.

VIOLATIONS OF AFAEA

- Criminal sanctions for willful violations and civil penalties may be imposed.

VIOLATIONS OF FARC

- International Emergency Economic Powers Act (IEEPA) Penalties
 - Civil penalty: may result in the institution paying a fine of up to \$295,141 per violation or twice the transactional value whichever is greater; and the individual may be fined up to \$295,141 per violation or twice the transactional value whichever is greater.
 - Criminal penalty: may result in the institution paying a fine of up to \$1,000,000 per violation; and the individual may be fined up to \$1,000,000- or twenty-year incarceration, or both per violation.

Additionally, for each violation, any or all of the following sanctions may be imposed:

- The denial of export privileges; and/or
 - The exclusion from exporting practice; and/or
 - Seizure/Forfeiture of goods.
- Trading with the Enemy Act (TWEA) Penalties (Cuba and North Korea)
 - Civil penalty: \$65,000 per violation
 - Criminal penalty: \$1,000,000 per violation and up to 10-year incarceration

RECORD KEEPING

ARE THERE SPECIFIC GUIDELINES FOR RECORD KEEPING OF EXPORT TRANSACTIONS?

ITAR

- Maintenance of Records by Registrants 22 CFR 122.5
- Recordkeeping for Exemptions 22 CFR 120.15

EAR

- Recordkeeping 15 CFR Part 762

FARC

- 31 CFR 501 Subpart C – Reports

Nuclear Regulations

- NRC: U.S. address, records, and inspections 10 CFR 110.53
- NNSA: Not specified in 10 CFR 810

WHAT RECORDS ARE REQUIRED TO BE KEPT?

In general, any paperwork detailing: internal export control assessments, including any documentation regarding the applicability of any licensing exemptions, license determinations, license submissions, post-license management, negotiations in connection with an export regardless of whether the export or re-export occurs.

HOW LONG ARE RECORDS REQUIRED TO BE KEPT?

Five years from last activity or expiration date.

HOW ARE RECORDS REQUIRED TO BE STORED?

Records must be kept in a way facilitates the ability to retrieve the records for any purpose and to review the records during internal or U.S. Government audits.

RESEARCH AND EDUCATIONAL ACTIVITIES

NATIONAL SECURITY DECISION DIRECTIVE 189 (NSDD189)

NSDD189 defined fundamental research to establish a national policy for “controlling the flow of science, technology and engineering information produced in federally funded fundamental research at colleges, universities, and laboratories”.

NSDD189 states: **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."

FUNDAMENTAL RESEARCH

ITAR definition of 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.

EAR definition of Fundamental Research

Research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted any restrictions for proprietary or national security reasons.

AFAEA definition of Fundamental Research

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.

Federal Policy Memos on Fundamental Research

DoD Memo May 24, 2010 (includes DoD Memo June 26, 2008 and NSDD189 Memo September 21, 1986=5)

FUNDAMENTAL RESEARCH EXCLUSION

Fundamental Research (as described in the regulations) is not subject to the regulations as proscribed under the ITAR definition of Public Domain Information, the EAR definition of Published Software and Information, and the AFAEA definition of Publicly Available Information.

ITAR (22 CFR § 120.34(8)), EAR (15 CFR § 734.3(b)(3)) and AFAEA (10 CFR Part 810.2(c)(2))

Remember: The Fundamental Research Exclusion may be void if the university or Principal Investigator accepts any of the following conditions (verbal and/or written), regardless of sponsor:

- prepublication review and approval;

- sponsor approvals or conditions on publication of information;
- foreign national controls or approvals;
- access and dissemination controls on the research;
- national security controls.

PUBLIC DOMAIN/PUBLICLY AVAILABLE INFORMATION

Not Subject to the ITAR, Public Domain (22 CFR § 120.34)

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

Not Subject to the EAR (15 CFR § 734.3(b)(3)) Information and “software” that:

- Are published* as described in 15 CFR § 734.7 (see below).
- Arise during, or result from, fundamental research, as described in § 734.8.
- Are released by instruction in a catalog course or associated teaching laboratory of an academic institution.
- Appear in patents or open (published) patent applications available from any patent office,

unless covered by an invention secrecy order, or are otherwise patent information at described in §734.10.

- Are non-proprietary system descriptions?
- Are telemetry data as defined in Note 2 to Category 9, Product Group E.

**Excludes certain encryption software – see ECCN 5D002*

Published 15 CFR § 734.7

a) Unclassified technology and software is published - and therefore not technology or software subject to the EAR - when it has been made available to the public without restrictions upon its further dissemination such as through any of the following:

- 1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;
- 2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;
- 3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;
- 4) Public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the Internet on sites available to the public; or
- 5) Submission of a written composition, manuscript, presentation, computer-readable dataset, formula, imagery, algorithms, or some other representation of knowledge with the intention that such information will be made publicly available if accepted for publication or presentation:
 - I. To domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers, or trade publications;
 - II. To researchers conducting fundamental research; or
 - III. To organizers of open conferences or other open gatherings.

b) Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in § 740.13(e) of the EAR.

AFAEA: (10 CFR Part 810.2(c)(2))

Publicly available information, publicly available technology, and the results of fundamental research.

EDUCATIONAL INFORMATION

Exclusions that allow for the teaching of commonly taught information to continue at universities.

EDUCATIONAL INFORMATION EXCLUSION EAR (15 CFR § 734.3(b)(3))

- focuses on venue.
- export controls do not apply to educational information conveyed in courses listed in course catalogs and associated teaching laboratories.
- does not cover encrypted software.
- this exclusion may be void if that same information is transferred to a foreign person outside of class.

GENERAL PRINCIPLES IN SCIENCE AND ENGINEERING ITAR (22 CFR § 120.33(b)):

- focuses on subject matter.
 - only covers general science, math and engineering principles commonly taught in schools, colleges, and universities.

EXEMPTIONS FOR EMPLOYEES

The use of an Employment Exemption requires the prior approval of an Export Compliance Officer. These employment exemptions are narrow in scope and applicability, require notification of the export to the employee and documentation of the process.

ITAR (22 CFR § 125.4(b)(10))

An exemption that applies to disclosures in the U.S. by U.S. universities of unclassified technical data to foreign nationals who are full time bona fide employees of the university. However, this exclusion may be void unless these conditions are met:

- the person must be a full-time, regular employee - post-docs, students and visiting researchers usually do not qualify;
- the employee must have a permanent U.S. residence during his or her period of employment;
- the employee is not a foreign national of an embargoed country;

- the university must notify the employee in writing that technical data cannot be transferred or re-exported to other foreign nationals without prior government approval.

EAR (15 CFR § 740.13)

Technology and Software Unrestricted (TSU) license exception that includes transfers in the U.S. by U.S. universities to their bona fide full time regular employees. Not all technology and software controlled under the EAR are eligible for this exception. There are also restrictions based on country of citizenship.

EXPORT CONTROL COMPLIANCE GUIDANCE

MYRESEARCH – EXPORT REVIEW QUESTIONS

The questions in myResearch are designed to assist in the identification of situations where an export license may be required and/or where activities might void the Fundamental Research Exclusion. It is important to note that there are activities that may require an export control license even though there are no sponsor restrictions, and the intent of the project is to publish and disseminate the findings.

ELECTRONIC COMMUNICATIONS (E-MAIL, FAX, AND SHARE DRIVES)

No export-controlled technical information should be sent via electronic means. Many mail servers store information in the cloud and there has been limited guidance from the federal government on whether storing information in the cloud is of itself an export. To err on the side of caution, it is best to avoid using electronic communications to convey export-controlled information and if it becomes absolutely necessary to do so, to utilize software that would encrypt the information.

SBU Google Apps for Education Acceptable Use and Data Security Policy

<https://it.stonybrook.edu/policies/d111>

ENCRYPTION

Encryption is a complex area of control under both the EAR and the ITAR. Any projects that involve strong cryptography should be reviewed in conjunction with the appropriate regulations.

[The Bureau of Industry and Security, Department of Commerce, provides extensive](#)

information on encryption, including classification tools.

<http://www.bis.doc.gov/index.php/policy-guidance/encryption>

FOREIGN PERSONS

The university is an “open” environment and welcomes foreign persons for participation in a variety of activities, such as educational, research, and recreational endeavors. To maintain compliance with the export regulations, the following items should be considered.

DEEMED EXPORTS

An export of technology or source code (except encryption source code) is ‘deemed’ to take place when it is released to a foreign person within the United States. It is important to determine if there is an export issue with research proposals/projects in which a foreign person will be assisting/collaborating, where third party proprietary data will be shared, or in situations where a software license agreement contains language indicating that the software is controlled to certain countries. As with other exports, technology that is publicly available is not subject to the deemed export rule, nor would the rule apply to fundamental research within an appropriate structure where any export-controlled information or technology would not be released to foreign persons on the project.

I129 EXPORT ATTESTATION REQUIREMENT

Form I-129 requires an Export Attestation for a foreign person on an H-1B, H-1B1 Chile/ Singapore, L-1 or O-1A visa petition, as follows:

With respect to the technology or technical data the petitioner will release or otherwise provide access to the beneficiary, the petitioner certifies that it has reviewed the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR) and has determined that:

- 1) A license is not required from either the U.S. Department of Commerce or the U.S. Department of State to release such technology or technical data to the foreign person;
or
- 2) A license is required from the U.S. Department of Commerce or the U.S. Department of State to release such technology or technical data to the beneficiary and the petitioner will prevent access to the controlled technology or technical data by the beneficiary until

and unless the petitioner has received the required license or other authorization to release it to the beneficiary.

VISITORS

Visitors come to campus for a variety of reasons, such as: to discuss or partake in research as consultants, collaborators, or visiting scholars, as part of delegations, for laboratory visits, to partake or present at conferences/lectures/seminars, for athletic or arts events, as hospital or campus volunteers. While not all visitors require an assessment of whether an export license would be required for the activities they will be engaged in, there are certain activities where there is a legal obligation or a due diligence obligation to review. These groups of visitors to campus should be screened against the various governmental restricted party lists to ensure compliance with U.S. laws and regulations. Furthermore, depending upon the access that the visitor might have, further documentation may be required to access whether an export license would be required.

SBU Guests/Visitor Policy: https://www.stonybrook.edu/policy/_pdf/guests_visitors_policy.pdf

International Visiting Scholars and Visiting Student Interns

Visiting Scholars and Visiting Student Interns may have access to research laboratories, including research equipment, research data, and on-going research projects. A review of the activities in conjunction with a review of access to facilities/information is required to ensure that an export license is not required for the Visitors participation in the proposed activities.

SBU Guests/Visitor Policy: https://www.stonybrook.edu/policy/_pdf/guests_visitors_policy.pdf

FOREIGN TRAVEL

Faculty, staff, and students must comply with United States' laws and regulations as well as Stony Brook University and the Research Foundation for SUNY's policies (as applicable) when traveling internationally on university business. Anyone traveling to foreign locations should enter their travel information into the appropriate on-line travel registry. Travel to certain destinations require prior approval.

SBU Travel Policy: https://www.stonybrook.edu/policy/_pdf/university_travel_policy.pdf

Laptops, PDAs, and Cell Phones

When traveling outside the U.S. with your laptop computer, PDA, cell phone, data storage

devices and/or encrypted software you may need an export license to take that equipment.

A laptop is generally an exception to the EAR and ITAR lists of controlled items/equipment.

However, this exception is **NOT** automatically allowed:

- A license is required when a laptop with controlled research data or encrypted/proprietary software is hand-carried or shipped abroad to a restricted country and/or to a denied person/entity.

For example: A laptop being hand-carried to any country with research data on a genetically modified organism will currently require a license genetically modified organisms are controlled items for chemical, biological and anti-terrorism reasons and there are no applicable license exceptions.

When hand-carrying a laptop, PDA, cell phone, data storage devices outside the U.S:

- You **MUST** always retain exclusive control of the equipment.
- You **MUST** not let the equipment be used by anyone in the foreign country.
- You **MUST** not intend to keep these items in these countries for longer than one year.
- You **MUST** verify that no government licenses are required.

Guidance from the Federal Bureau of Investigations for international travel:

<https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view>

<https://www.fbi.gov/file-repository/student-travel-brochure-pdf.pdf/view>

Guidance from the Division of Information Technology: <https://it.stonybrook.edu/help/kb/it-security-considerations-while-traveling>

Field Equipment

Traveling outside the U.S. with your field equipment and/or shipping your field equipment to your research site may require an export license. If the item/technical information is subject to ITAR (on the USML list), the export will require a license regardless of destination. If the item/technical information is subject to EAR (on the CCL), the export details need to be reviewed to determine if there is an applicable license exception or if a license is required. As per the regulations, the steps in determining whether a license is required and/or the application of a license exception need to be recorded.

OFAC Sanctioned Countries

Anyone traveling to OFAC sanctioned countries should work with the Export Compliance Officer

prior to traveling to ensure compliance with all export control laws.

OFAC Sanction List is available at: <https://ofac.treasury.gov/sanctions-programs-and-country-information>

Presenting at Conferences/Workshops

Faculty presenting at conferences or meetings overseas are responsible for understanding export laws and regulations and how they apply to their respective disciplines and/or situations. If any controlled information, technology, software, or equipment will be transferred to a foreign party overseas, a license may be required prior to the transfer unless a valid licensing exception or exclusion applies.

In general, if you are presenting at a conference that will be open* to anyone and the information to be presented *is* already published (ITAR) or is information that *will be* published (EAR) a license should not be required. It is highly recommended that the presenter ensure that they comply with export controls whenever releasing information to third parties – any questions should be directed to the Export Compliance Officer.

*A conference is considered “open” if all technically qualified members of the public are eligible to attend and attendees are permitted to take notes or otherwise make a personal record (but not necessarily a recording) of the proceedings and presentations. In all cases, access to the information must be free or for a fee that does not exceed the cost to produce and distribute the material or hold the conference (including a reasonable profit).

INTERNATIONAL COLLABORATIONS

The University enters into collaborations with international entities for a variety of reasons, such as academic (student) exchange programs, scholar exchange programs, research collaborations, satellite campuses. These collaborations are usually memorialized in an agreement, whether there is an exchange of funds, and should be reviewed and signed by the appropriate authorized campus official.

MEMORANDUM OF UNDERSTANDING (MOU)

MOUs should be reviewed by all offices that are impacted and/or are committing of resources in the agreement. MOUs should be reviewed for export control compliance through a restricted parties screening, determination of whether any export licenses are

required for the exchange of information and/or physical shipments.

PROPRIETARY INFORMATION

Third party proprietary information, information that is not in the public domain, is not excluded from export control regulations even if it is received in conjunction with a fundamental research project. ***Non-Disclosure Agreements (NDAs)*** should be utilized for exchange of information that may include receipt of outside proprietary information and/or divulging university proprietary information (i.e., pending patent applications that are not yet published). An NDA will require that a company/sponsor identify any export controlled proprietary information, this important step will allow the university to determine if an export license would be required to share the information with a foreign national. Economic Development can assist with NDAs.

PUBLICATION/FOREIGN PERSON RESTRICTIONS

State University of New York policy prohibits the acceptance of any awards that restrict dissemination of research results ([Document 1800](#)) and/or foreign person participation ([Document 1801](#)). Requests for justifiable exceptions to this policy, on a case-by-case basis, such as for the purpose of protecting state and national security, must be submitted to the Export Compliance Officer for submission for Chancellor or designee authority's approval. Any projects that are granted exceptions to these SUNY policies will be further reviewed for the need of a technology control plan and/or export licenses.

RECEIPT OF MATERIALS, EQUIPMENT, TECHNOLOGY AND TECHNICAL INFORMATION/DATA

Classification

Purchasing, renting/leasing, borrowing, or any other transfer of supplies, equipment, and/or technical information/data from an outside party to campus should be accompanied by an export control classification number (EAR) or item designation (ITAR) as applicable. Whenever receiving items subject to the export control regulations, the Export Compliance Officer should be notified to determine if a Technology Control Plan is needed. If you are renting or borrowing equipment, please consult with the Office of Sponsored Programs to have an Equipment Loan

Agreement completed to protect yourself, your laboratory, and the institution.

Vendor Screening

A screening should be completed on all vendors, especially foreign vendors, to confirm that they are not on any of the restricted parties list – this is particularly important in ensuring that OFAC violations do not occur.

P-Cards and Credit Cards

When utilizing P-cards and credit cards, it is the user's responsibility to acquire the export classification of any items purchased as well as determining that there are no federal restrictions on utilizing the selected vendor.

SHIPPING: SENDING MATERIALS, EQUIPMENT, TECHNOLOGY, AND TECHNICAL INFORMATION

Sending Materials

University created materials, technology, technical information, and/or data. The Fundamental Research Exclusion pertains to the **information** resulting from fundamental research projects; it does not pertain to the tangible products of the fundamental research projects. The tangible products, i.e., prototypes, materials, some software, genetically modified organisms, need to be evaluated in accordance with the regulations to determine if an export license or documentation of an export license exception is required.

Materials, including biologics and chemicals, being shipped off campus need to be reviewed by Intellectual Property Partners in consultation with Environmental Health & Safety to ensure proper handling of the materials and for the determination of whether an agreement is required. In some instances, a Material Transfer Agreement (MTA) should be utilized to protect university/faculty intellectual property and/or to prevent re-export (re-transfer) of material being shipped.

Before Shipping Checklist for Export Compliance

Is the item controlled under the export control regulations?

- Yes, and it is controlled under the International Traffic in Arms Regulations (ITAR) – STOP - an export license is required.
- Yes, and it is controlled under the Export Administration Regulations (EAR) – STOP – is an

export license required for the destination you are sending the item to or is there a license exception.

Does the person or entity that you are sending the item appear on any restricted party lists? Is it a legitimate end purpose?

U.S. Census Bureau Requirement for International Shipments

International shipments may require that an Electronic Export Information (EEI) be filed with the U.S. Census Bureau. The EEI is now filed electronically through the Automatic Export System (AES).

- The EEI must be prepared regardless of value for all shipments requiring an export license.
- Destination statement should appear on any items subject to US control – “These commodities, technology, or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to US law is prohibited.”
- The EEI must be prepared for shipments when the shipment through U.S. Postal Service (USPD) is valued over \$500. EEIs are required for shipments not using the USPS when the value of the commodities classified under any single schedule B number is over \$2,500. If no EEI is required, the airway bill or other loading document should state “No EEI required - no individual Schedule B number valued over \$2,500.”
- A copy of the EEI documentation should be provided to the Office of Sponsored Programs or Office of Technology Licensing and Industry Relations, as appropriate.
- Intangible exports of technology controlled under Commerce (EAR 99) do not require an EEI. (15 CFR 30.55(o)).

SERVICE CENTERS (IFRS AND S&FS)

Activities undertaken by laboratories/centers when functioning as an IFR or S&F are not considered fundamental research or educational. As such, all incoming export-controlled materials from outside entities must be identified as such by the senders prior to acceptance by the service center. The service center is responsible for notifying the Research Security Program of the intent to receive said materials for review of the need for either an export license or technology control plan. Furthermore, if export- controlled equipment, supplies and/or technical information/data is utilized in this space, a Technology Control Plan should be

developed with the Research Security Program.

TECHNOLOGY CONTROL PLANS

A Technology Control Plan (TCP) is required for all research work involving an ITAR or EAR export issue or any other restrictions (publication, foreign person restrictions) that remove the work from the Fundamental Research Exemption. The TCP shall include a physical and information security plan, personnel screening procedures and a process for conducting the research in a controlled environment. The TCP will document compliance with the contract terms and conditions and contains at a minimum the following elements:

- RF project number and title, if applicable
- PI name and department/laboratory
- Research location (laboratory/building)
- Sponsor name & contract number
- Brief statement of need for plan
- Description of plan for protection of technology
- Project Director/Principal Investigator signature
- Empowered Official signature

INTERNAL EXPORT CONTROL COMPLIANCE ROLES AND RESPONSIBILITIES

WHO PARTICIPATES IN A COMPLIANCE PROGRAM?

An effective export compliance program necessitates participation and coordination of multiple parties in the export review process. Researchers may be held personally liable for violations of the export regulations and should exercise care in completing any required forms and/or questions.

ESCALATION PROCESS

Any export control issues or known violations should be reported immediately to the Office of the Vice President for Research , per the campus [Confidential Export Control Escalation Policy](#).

LEGAL COUNSEL

SUNY, RF, and SBU provide general export compliance guidance to the Office of the Vice-

President for Research, the Director of Research Security and the Export Compliance Officer. RF maintains a system-wide export control website, whereas a campus level website is maintained by the Office of the Vice-President for Research.

EXPORT COMPLIANCE PROGRAM

Office of the Vice-President for Research (OVPR)

The OVPR has been delegated University wide authority for export control compliance. The Director of Research Security (Research Security Program) within the Office of the Vice-President for Research is designated as the responsible party for the oversight of an export compliance program.

Vice President for Research (VPR)

The VPR is the authorized University official for the University's export control program. Technology control plans, commodity jurisdiction requests, export license applications, and any other request to a federal agency regarding export controls, as well as any requests for publication and/or foreign national waivers, must be authorized by the VPR or his/her designee.

Research Security Program

The Research Security Program is responsible for the oversight of SBU's Export Control Compliance Program.

Director of Research Security (DRS)

The DRS serves as the VPR's designee for SBU's Research Security Program,

The DRS (in addition to the VPR) is the Empowered Official for SBU. According to 22 C.F.R. § 120.25, the Empowered Official is a U.S. person who:

- 1) Is directly employed by the applicant or a subsidiary in a position having authority for policy or management within the applicant organization; and
- 2) Is legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of the applicant; and
- 3) Understands the provisions and requirements of the various export control statutes and regulations, and the criminal liability, civil liability, and administrative penalties for violating the Arms Export Control Act and the International Traffic in Arms Regulations; and
- 4) Has the independent authority to:

- (i) Inquire into any aspect of a proposed export or temporary import by the applicant;
and
- (ii) Verify the legality of the transaction and the accuracy of the information to be submitted; and
- (iii) Refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

Export Compliance Officer (ECO)

The University official responsible for the University's export compliance program. The ECO assists academic and administrative offices in the development of policies and guidance documents to ensure compliance with the export control laws and this policy. The ECO:

- Assists principal investigators in the assessment of possible export control issues;
- Facilitates requests for licenses;
- Documents license exemptions and exceptions;
- Creates Technology Control Plans;
- Trains principal investigators and department administrators in export controls.

Research Security Working Group (RSWG)

- A committee chaired by the Director of Research Security that includes members of administrative offices that have some responsibility for export compliance. The RSWG assists in the evaluation and maintenance of the University's posture for compliance with federal government export control regulations.

CAMPUS OFFICES

Office of Sponsored Programs (OSP)

OSP is charged with all pre-award activities for Stony Brook University. This includes proposal preparation, review, and endorsement; contract review negotiation and approval; support and guidance to the campus-based foundation (Stony Brook Foundation) on sponsored program issues; and the establishment of funded awards in the Oracle enterprise financial system. At the pre-award stage, OSP reviews program announcements (or requests for proposals) and the myResearch export control questions to identify any potential export control issues and/or restricted parties. If any potential export control issues are identified at the time of the

proposal submission, OSP shall notify the Export Compliance Officer for further review. At the award stage, OSP reviews the award document for restrictions and/or language to ensure that the fundamental research exemption is maintained. If any potential export control issues are identified at the time of award, OSP shall notify the Research Security Program for further review and approval prior to award acceptance.

Office of Grants Management (OGM)

OGM helps Principal Investigators, Project Directors, and their staff to manage the project by monitoring financial activity according to sponsor terms and conditions. OGM completes denied party screenings on non-employee payments to individuals. Any issues or red flags are brought to the Research Security Program for further review.

Economic Development

Intellectual Property Partners (IPP) is responsible for management of the university's intellectual property portfolio. IPP negotiates license, material transfer agreements and non-disclosure agreements. IPP completes restricted party screenings, assists faculty with export classifications prior to sending materials, and reviews potential exchanges/collaborations for any other potential export control considerations. Any issues or red flags are brought to the Research Security Program for further review.

Audit –RESERVED

Environmental Health and Safety (EH&S)

EH&S promotes safety and environmental stewardship through the development and implementation of a variety of environmental, health and safety programs.

Human Resources (HR)

HR provides an array of HR campus services such as recruitment, appointment, payroll, benefits, training, labor relations, and record keeping. HR reviews new employees against the denied parties lists and assists in developing processes to red flag potential new employment opportunities for export control issues. Any issues or red flags are brought to the Research Security Program for further review.

Division of Information Technology (DoIT)

DoIT supports the academic, research, healthcare, and administrative missions of Stony Brook University by providing the necessary infrastructure to support network connectivity,

telecommunications, data storage; as well as innovative services, systems, applications, and training to assist students, faculty, staff, and researchers in their work.

International Academic Programs and Services (IAPS)

IAPS provides an array of international campus services such as student exchange programs, non-sponsored international travel, advises and assists with visa services for student, faculty, and visitors. IAPS hosts the non-sponsored international travel registration system to include declaration of items being taken abroad. IAPS hosts the VIS system for processing DS2019 requests including a review for denied parties and export concerns.

Procurement - RESERVED

Procurement provides purchasing, accounts payable, shipping & receiving, and property control services to the campus community.

FACULTY AND STAFF

Deans and Chairs

Knowledge of export control regulations: Deans and chairs should be familiar with the information provided in this manual, the information on SBU's export control website, the information on the State University of New York and the Research Foundation of State University of New York's export control website and the export controls as they relate to the area(s) of research that are under their purview. Any red flags, concerns, or questions should be reported to the Research Security Program for further review.

Principal Investigators

Knowledge of export control regulations: Principal Investigators should be familiar with the information provided in this manual, the information on SBU's export control website, the information on the State University of New York and the Research Foundation of State University of New York's export control website and the export regulations as they relate to their area of research, shipping, and sharing information.

Assist the Research Security Program in the Assessment of Possible Export Control Issues:

Principal Investigators should assist campus offices in assessing the possibility of export control issues by completing the Export Control Questions in myResearch Grants and as applicable the License Assessment Form to the best of their knowledge and seeking assistance from the

appropriate campus office when additional information is needed to complete these forms.

Assist the Research Security Program in Commodity Jurisdiction Requests, License Requests, and Voluntary Disclosures: Principal Investigators should assist the Research Security Program in obtaining all the required information to facilitate the expedient and accurate completion of Commodity Jurisdiction Requests, License Requests, Voluntary Disclosures and Technology Control Plans.

University Staff

Knowledge of export control regulations: University staff should be familiar with the information provided in this manual, the information on SBU's export control website, the information on the State University of New York and the Research Foundation of State University of New York's export control website and the export regulations as they relate to their area of responsibility.

Assist the Research Security Program: University staff should follow all formal procedures that are disseminated for their area of responsibility. Any red flags, concerns, or questions should be reported to the DRS for further review.

EXPORT REVIEW PROCESS, CLASSIFICATIONS, LICENSE EXCEPTIONS AND LICENSES

EXPORT REVIEW PROCESS

Export control regulations are complex and situational. Due to these factors, the determination for one project cannot be readily applied to another project. The university is continuously reviewing its export control compliance program and implementing new processes/procedures to ensure compliance and educate university administrators, faculty, and staff. To best mitigate the university's risk for non-compliance, it is strongly encouraged that the following types of activities follow the proscribed review/approval chains. If you have a situation that is not addressed below or in this document, contact the Research Security Program.

The Research Security Program has provided [Guidance and Procedure Documents](#) to assist the Campus Community in complying with export control regulations.

Foreign Travel: if you plan to take items other than your "clean" laptop (no export controlled or

proprietary information), cell phone, or data storage device, contact the Research Security Program. If you are taking your laptop, cell phone, or data storage device, make sure that you are familiar with the terms of the TMP license exception and the import/customs regulations of the country you will be visiting.

Foreign Visitors: if you plan to host foreign visitors that are not coming to the university on a university sponsored visa, contact the Export Compliance Officer.

Material Transfers: all transfers of investigator-created/modified materials being shipped off-campus should be reviewed by Intellectual Property Partners (IPP) for export control issues and whether a Material Transfer Agreement is required. Please note that if appropriate, Environmental Health & Safety should be consulted for proper shipment of hazardous materials.

Memorandums of Understanding: all MOUs (and other similar types of agreements) with international entities should be reviewed by the Export Compliance Officer for an export review of the proposed collaboration.

Proprietary Information: if you will be receiving proprietary information, be aware that this information may be export controlled. When accepting proprietary information from companies it is advantageous to have a Non-Disclosure Agreement (NDA). An NDA can be facilitated by Intellectual Property Partners/Economic Development.

Research: all research projects (funded and non-funded) should be submitted to the Office of Sponsored Programs via a myResearch Grants application which initiates an export review of the project.

Purchasing: if you are purchasing items, you should ask the vendor if the item is export controlled. If your item is export controlled, you should contact the Research Security Program for further guidance.

Shipping: all international shipments should be reviewed for export compliance, including a restricted party screening. According to export control record keeping regulations - a record of the determination of whether an item is controlled and if so, whether a license is required should be documented. If it is not clear that your item is not regulated, contact the Research Security Program.

ITEM/TECHNOLOGY CLASSIFICATION

What are the steps to determine if an item/technology is controlled?

In determining if your item/technology (“item”) is controlled under the export regulations, the following steps should be followed:

- 1) United States Munitions List
 - Is my item specifically enumerated on the United States Munitions List?
 - If my item is not specifically enumerated, is it nevertheless “caught” or “held” as an item specifically enumerated in the list?
- 2) Is my item under the control of another agency, Treasury Department, Office of Foreign Asset Control, U.S. Nuclear Regulatory Commission, Department of Energy, Patent and Trademark Office, or Department of Defense (DoD) Department of State Foreign Military Sales Program?
- 3) Commerce Control List – “600 Series” ECCNs
 - Is my item specifically enumerated on the Commerce Control List?
 - If my item is not specifically enumerated, is it nevertheless “caught” or “held” as an item specifically enumerated in the list?
- 4) Commerce Control List – other than 600 Series

The term “specially designed” defined in ITAR § 120.41 and EAR § 772.1 is based around the fishing practice of “catch” and “release.” Sub-paragraphs (a)(1) and (a)(2) in both definitions “catch” items, but then there are several subsequent (b) sub-paragraphs that may “release” particular items if they satisfy any one of the enumerated criteria.

Commodity Jurisdiction Requests

When it is unclear whether an item and/or technology falls under jurisdiction of the Department of State (ITAR) or the Department of Commerce (EAR), a Commodity Jurisdiction Request can be submitted through the Export Compliance Officer to the Office of Defense Trade Controls. (See 22 CFR 120.3 and 120.4).

Classification Requests

When it is unclear what an item/technology’s appropriate classification is under the EAR, a Classification Request can be submitted to the Bureau of Industry Standards through the Export Compliance Officer. If it is unclear if a license is required for a particular transaction, a request

for an advisory opinion can be submitted to the Bureau of Industry Standards through the Export Compliance Officer.

LICENSE EXCEPTIONS

International Traffic in Arms Regulations (ITAR)

Under the ITAR, license exceptions are extremely limited, and no item enumerated on the United States Munitions List should be exported without consultation with and approval from the Export Compliance Officer.

Export Administration Regulations (EAR)

Under the EAR, Section 740.1 through Section 740.20 a license exception is an authorization that allows you export or re-export under specific guidelines items subject to the EAR that would otherwise require a license.

Note:

- Not all license exceptions are applicable to all items on the EAR.
- Even if stipulated as a license exception for an item it may not be applicable for all destinations.
- All license exceptions need to be recorded as to how the determination of applicability was made.

LICENSES

Only the designated empowered official may apply for a license. License determinations depend on the specifics of each transaction and the regulatory agency. Consultation with the Export Compliance Officer should be made prior to sharing or shipping any export-controlled items internationally (including Canada).

To facilitate a review of the export transaction, the following information should be made available to ORC:

- What is being shipped?
- What country is the item being shipped to?
- To whom is the item being shipped?
- What is the intended use of the item?

Depending upon the details of the export transaction and the regulatory agency involved,

licenses can take up to six months to receive.

VOLUNTARY DISCLOSURE

If after reviewing the export compliance information provided in this manual and/or any of the supporting documents and/or websites, it is believed that an export violation may have occurred, please contact the DRS. They will work in conjunction with the principal investigator to determine if a violation has occurred; and if required will coordinate with the Vice- President for Research to file a voluntary disclosure to the appropriate agency.

Department of State: The Department of State strongly encourages the disclosure of information to the Directorate of Defense Trade Controls (DDTC) by persons, firms, or any organization that believes that they may have violated the International Traffic in Arms Regulations. Voluntary self-disclosure may be considered a mitigating factor in determining the administrative penalties, if any, that can be imposed by the Department of State.

Department of Commerce: The Department of Commerce encourages the disclosure of any violation of the Export Administration Regulations to the Office of Export Enforcement (OEE). Disclosure to OEE prior to the time that OEE, or any other agency of the U.S. government, has learned the same, or substantially similar information, is considered a mitigating factor in determining what administrative actions, if any, will be sought by the OEE.

Department of Treasury: The Department of Treasury encourages the disclosure of any violation of Office of Foreign Assets Control (OFAC) regulations to OFAC. Self-disclosure is considered a mitigating factor in civil penalty proceedings.

AUDIT INTERNAL ASSESSMENTS

The internal assessment function is designed to objectively and independently review all aspects of the export control program. Internal assessments will be conducted at the campus level as required, and will include:

- Regular internal audits will be conducted to ensure that the Export Control Compliance Program is operating effectively, guidelines are being followed and that processes are updated as needed and/or required.

- A review of select contracts, grants, activities, practices, and procedures will be conducted to assess whether export control policies and procedures are being successfully implemented.

TRAINING AND EDUCATION

Stony Brook University is committed to ensuring that export control training information is disseminated throughout the campus. The Office of the Vice-President for Research has the following training opportunities available to the campus community:

Collaborative Institutional Training Initiative (CITI): provides a general export overview module as well as specific areas of compliance (e.g. biosafety, operational departments, international shipping, purchasing), The CITI modules are available to all Stony Brook University faculty, staff, and students at <https://www.citiprogram.org/>

Descartes Visual Compliance: one-on-one meeting to assist principal investigators in item classification through the interactive use of eCustoms Visual Compliance.

Internal Resources:

- Stony Brook University website:
<https://www.stonybrook.edu/commcms/export-controls/index.php>
- The Research Foundation for SUNY website: <http://www.rfsuny.org/Our-Work/Sponsored-Programs-Administration/Sponsored-Programs-and-Research-Compliance/Export-Controls/>

External Resource Lists:

- U.S. Department of State:
https://www.pmdotc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing
- U.S. Department of Commerce, Bureau of Industry Standards:
<http://www.bis.doc.gov/index.htm>
- BIS On-line Training Room: <https://www.bis.doc.gov/index.php/online-training-room>
- Chemical and Biological Controls - Bureau of Industry and Security
<https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/chemical-and-biological-controls>

biological-controls

- Encryption - Bureau of Industry and Security

<https://www.bis.doc.gov/index.php/encryption-and-export-administration-regulations-ear>

- U.S. Department of Treasury: <http://www.ustreas.gov/offices/enforcement/ofac/>