I. INTRODUCTION

This paper summarizes the primary legal and regulatory regimes controlling the transfer of items, technology and services to foreign nationals, and highlights some of the key regulatory issues confronting such transfers in the context of university research.

Just as commerce has become global in scope, university research increasingly involves global collaboration and exchange of information and technology. University research activities involve graduate students, researchers and other professionals who are foreign persons, and may also be conducted in collaboration with private businesses employing foreign persons or based abroad. However, at the same time, university research often involves items, technology or technical data which may not be freely shared with all foreign persons under U.S. export control laws.

Like all U.S. persons and entities, universities and their representatives must comply with U.S. export control laws, and will be held accountable for noncompliance. The burden of compliance is never more challenging than with respect to the transfer of controlled items, technology and technical data to foreign nationals who are students, professional colleagues, and research collaborators. Compliance may challenge the very essence of a university’s mission to foster the collaborative exchange of information and ideas. Judging research collaboration and information exchange, not by common interest and academic worthiness, but by the national origin of one’s colleagues can seem antithetical to the university’s mission.

How, then, can universities fulfill their legal obligation to prevent and uncover violations of export controls which may occur in the course of research, while still maintaining their traditional values? Fortunately, successful compliance with U.S. export control laws is possible – without sacrificing the university’s important mission – with a thorough understanding of applicable laws and regulations, and how they apply within the university community.

II. LEGAL AND REGULATORY OVERVIEW

United States export control laws and regulations control the export of articles, services and related technical data, including the transfer of such items to foreign persons. The
export regimes impose licensing and other requirements predicated on a general
distinction between “U.S. persons” and “foreign persons (or nationals)”.

A. The International Traffic in Arms Regulations

Under the Arms Export Control Act (“AECA”), 22 U.S.C. § 2778, the U.S.
Department of State (“DoS”), Directorate of Defense Trade Controls (“DDTC”),
is responsible for implementing and enforcing the International Traffic In Arms
Regulations (“ITAR”), 22 C.F.R. §§ 120-130.

1. What is Controlled under the ITAR?

a. The ITAR control the export of defense articles, defense services,
and related technical data from the United States to foreign
destinations and persons.

b. A “defense article” is defined as “any item or technical data
designated in § 121.1 of this subchapter [ITAR]. . . and includes
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. . . [but] does not
include basic marketing information on function or purpose or
general system descriptions.” ITAR § 120.6. Section 121.1 is the
United States Munitions List (“USML”). To the extent university
research involves the development or transfer of items listed on the
USML, items adapted or conformed for a defense purpose, or
technical data related to such items, the research activities are
subject to the ITAR.

c. The term “technical data” is broadly defined and includes “(1)
[i]nformation, other than software. . .which is required for the
design, development, production, manufacture, assembly,
operation, repair, testing, maintenance or modification of defense
articles. . .[including] blueprints, drawings, photographs, plans,
instructions and documentation. . . (2) [c]lassified information
relating to defense articles and defense services. . . (3)
[i]nformation covered by an invention secrecy order. . . (4)
[s]oftware . . .directly related to defense articles. . . (5) . . .[but not]
information concerning general scientific, mathematical or
engineering principles commonly taught in schools, colleges and
universities or information in the public domain . . .[or] basic
marketing information on function or purpose or general system
descriptions of defense articles.”

d. In addition, any article (including technical data) may be
determined to be a “defense article”, although not specifically
listed on the USML, if it “(a)[i]s specifically designed, developed,
configured, adapted, or modified for a military application, and (i) [d]oes not have predominant civil applications, and (ii) [d]oes not have performance equivalent (defined by form, fit and function) to those of an article or service used for civil applications. . .” Similarly, an article or service may be determined to be a “defense article” or “defense service” if it “[i]s specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability such that control under this subchapter is necessary.” ITAR § 120.3.

NOTE: the intended use of an article or service after export – that is, whether it is intended for a military or civilian purpose – is not determinant of whether that article or service is controlled as a “defense article”. Id.

e. The term “defense services” is broadly defined as “[t]he 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,” or “the furnishing to foreign persons of any technical data controlled under this subchapter ... whether in the United States or abroad.” ITAR § 120.9.

2. What is not Controlled under the ITAR?

a. As noted, information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities, and information which is in the public domain, are excluded from ITAR control. ITAR § 120.10.

b. Information is considered to be in the public domain when it is generally accessible or available to the public through: sales at newsstands and bookstores; subscriptions available without restriction; distribution at conferences open to the public; patents available at any patent office; second-class mailing privileges granted by the U.S. Government; libraries open to the public or from which the public can obtain documents; public release or unlimited distribution following approval of a sponsoring U.S. Government agency or department; or, particularly significant for universities, fundamental research. ITAR § 120.11.

3. What is Fundamental Research under the ITAR?
a. Fundamental research refers to basic and applied research in science and engineering at accredited institutions of higher learning in the U.S., but only where the resulting information is ordinarily published and shared broadly in the scientific community. ITAR § 120.11(8). Fundamental research is considered to be in the public domain and exempt from ITAR export controls.

b. The fundamental research exemption under the ITAR does not include research the results of which are subject to any restrictions placed on access or dissemination, whether as a result of proprietary rights restrictions or specific U.S. government controls. Access or dissemination restrictions may deprive information of fundamental research status under the ITAR which would otherwise be eligible for that status if controlled under the Export Administration Regulations, as discussed below.

c. Information released to the University by a third party, such as a government or commercial sponsor, is not within the fundamental research exemption because it does not arise during or as the result of fundamental research. Unless exempt from controls for some other reason, third party information related to a defense article is ITAR-controlled information. If released to a foreign person, both the sponsor and the University are at risk of violating ITAR prohibitions against unauthorized exports.

d. The fundamental research exemption does not cover related technical assistance or services provided to a foreign person – only the act of furnishing the technical data to that person. A license must be obtained from DDTC before rendering any assistance or service related to the fundamental research provided to a foreign person.

4. Who is a “U.S. Person” under the ITAR?

a. A “U.S. person” is defined under the ITAR as a “. . .lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or [one] who is a protected individual as defined by 8 U.S.C. 1324b(a)(3) . . . [including] any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States . . . [as well as a U.S.] governmental (federal, state or local) entity . . . [but] does not include any foreign person. . .” ITAR § 120.15.

b. The term “lawful permanent resident”, as defined by 8 U.S.C. 1101(a)(20), means a person with “. . .the status of having been lawfully accorded the privilege of residing permanently in the United States of America under this chapter.” ITAR § 120.15.
United States as an immigrant in accordance with the immigration laws. . .”

c. The term “protected individual” is defined by 8 U.S.C. 1324b(a)(3) to include:

i. a citizen or national of the United States; or

ii. an alien (1) lawfully admitted for permanent residence, (2) granted the status of an alien lawfully admitted for temporary residence under certain “amnesty” provisions no longer currently available, (3) admitted as a refugee based on humanitarian concerns, or (4) granted asylum – but only if both of the following conditions are met:

- The alien applies for naturalization within six months of the date s/he first becomes eligible; and

- The alien has been naturalized as a citizen within two years after the date of her or his application for naturalization, or if not, can establish active pursuit of naturalization.

5. Who is a Foreign Person under the ITAR?

A “foreign person” is effectively defined under the ITAR to be a person who is not a U.S. person. Thus, a “foreign person” means “any natural person who is not a lawful permanent resident. . .or. . .a protected individual . . .[as defined under U.S. immigration laws, 8 U.S.C. 1101(a)(2), 1324b(a)(3), discussed above]. . .[and] 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 United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g. diplomatic missions).” ITAR § 120.16.

6. What is an “Export” under the ITAR?

a. Under the ITAR § 120.17, an export has occurred when –

i. a defense article has been sent or taken out of the United States in any manner, except when a person merely travels outside of the United States with personal knowledge which includes controlled technical data;
transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether in the United States or abroad;

disclosing (including any form of oral or visual disclosure) or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government, such as diplomatic missions;

disclosing (including any form of oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or

performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.

b. A “reexport” occurs under the ITAR when a defense article or defense service is transferred “. . .to an end use, end user or destination not previously authorized.” ITAR § 120.19.

7. **ITAR Requirements**

a. The ITAR require exporters to comply with registration, licensing, recordkeeping, and reporting provisions. DDTC is vested with broad discretion to determine, under subjective standards, whether ITAR compliance requirements are satisfied.

b. Any exporter subject to the ITAR must register and obtain license approval for the export of articles, technology, technical data, or technical services controlled on the USML prior to shipment or transfer. The process includes completing an export license application, researching the *bona fides* of the end-user, confirming the use to which the export will be put, and submitting certifications regarding the method through which the business was obtained. DDTC will issue a license, with any limitations appended ("provisos"), valid for a specified period of time (e.g., 24 months, 48 months). An exporter must maintain export records for a minimum of five years in a manner readily accessible to the U.S. Government for review.

c. The U.S. Government views compliance with export control laws seriously. Violations of the ITAR - as well as EAR, antiboycott, and embargoed countries/persons prohibitions described later - may result in the imposition of criminal or civil penalties, in addition to the suspension or denial of exporting privileges. Recent cases indicate that the conviction rate under these laws and regulations remains high, and that judges comply strictly with the
Federal Sentencing Guidelines in imposing sentences against individuals and entities convicted of violations.

8. **Exemptions from ITAR Requirements**

a. The ITAR exempt from licensing requirements certain exports of defense articles, technical data, and/or defense services as specified in ITAR §§ 123.16, 125.4 and part 126. These exemptions do not apply to exports to countries for which special embargoes or sanctions apply, or to nationals of those countries. Also, these exemptions may not be used to export technical data intended to aid offshore procurement arrangements or production of defense articles offshore.

b. The following exemptions are applicable specifically to universities:

i. unclassified technical data disclosed in the U.S. by U.S. institutions of higher learning to foreign persons who are their *bona fide* and full time regular employees, but only if (1) the employee’s “permanent abode” is in the United States during the period of employment, (2) the university informs the employee in writing that the information may not be transferred to other foreign persons without DDTC’s prior written approval, and (2) the employee is not a national of an embargoed country;

ii. exports by an accredited institution of higher learning of articles fabricated only for fundamental research purposes otherwise controlled by USML Category XV (a) (spacecraft, including communications satellites, remote sensing satellites, scientific satellites, research satellites, navigation satellites, experimental and multi-mission satellites) and (b) (ground control stations for telemetry, tracking and control of spacecraft or satellites, or employing cryptographic items controlled under Category XIII of the USML), but only if these conditions are present:

- The export is to an accredited institution of higher learning, a governmental research center, or an established government funded private research center located within NATO countries, countries designated as a major non-NATO ally, or member countries of the European Space Agency or the European Union, and involves nationals of such countries.
• All of the information about the articles, including design information and information obtained through fundamental research involving the article will be published and shared broadly within the scientific community, and is not restricted for proprietary reasons or specific U.S. government access and dissemination controls or other restrictions accepted by the institution or its researchers on publication of scientific and technical information resulting from the project or activity.

• If the article is to be permanently exported, the satellite into which the article will be incorporated must be a scientific, research, or experimental satellite, be exclusively concerned with fundamental research, and only be launched into space from the above countries and by their nationals.

iii. exports by an accredited institution of higher learning of defense services for the items identified in section ii above, if the following conditions are met:

• The exports will be to the same countries as specified for the items identified above, and exclusively to nationals of such countries when engaged in international fundamental research conducted under the aegis of an accredited U.S. institution of higher learning.

• The services will directly support fundamental research conducted by an accredited U.S. institution of higher learning or an accredited institution of higher learning, a governmental research center or an established government funded private research center located within these countries.

• Discussions will be limited to assembly of the items described in section ii above, and/or integrating such article into a scientific, research, or experimental satellite.

• This exemption does not cover discussions involving launch activities, including the integration of the satellite or spacecraft to the launch vehicle; information controlled under the Missile Technology Control Regime, discussed below, or classified as significant
military equipment; or, the transfer or access to technical data, information, or software otherwise controlled as classified information.

c. Other exemptions which are possibly of significance to university research activities include the following:

i. defense articles and related technical data, but not most defense services, exported to Canada when for end-use in Canada by Canadian Federal or Provincial governmental authorities acting in an official capacity or by a Canadian-registered person;

ii. technical data, including classified information, to be disclosed to a foreign person pursuant to an official written request or directive from the U.S. Department of Defense (“DoD”);

iii. unclassified models or mock-ups of defense articles, provided that such models or mock-ups are non-operable and do not reveal any technical data in excess of that which is exempt under other exemptions, discussed below, and do not contain components covered by the USML (to-scale models or mockups can reveal technical data beyond that which is authorized by this exemption);

iv. defense articles and technical data, including classified information, in furtherance of an agreement, such as a technical assistance agreement, approved by DDTC, with certain conditions, such as compliance with provisos and limitations placed on the authorized agreement;

v. technical data, including classified information, in furtherance of a contract between the exporter and a U.S. Government agency, but only if the contract provides for the export and the exported technical data does not disclose the details of design, development, production or manufacture of any defense article;

vi. copies of technical data, including classified information, previously authorized for export to the same recipient;

vii. technical data, including classified information, in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export to the same recipient, except that intermediate or depot-level repair and maintenance information may only
be exported under a license or agreement approved specifically for that purpose;

viii. technical data, including classified information, for which the exporter has received a written exemption by DDTC pursuant to an arrangement with DoD, the Department of Energy, or the National Aeronautics & Space Administration requiring such exports;

ix. technical data, including classified information, being returned to the original source of import;

x. technical data approved for public release, *i.e.* unlimited distribution, by the cognizant U.S. Government department or agency or Directorate for Freedom of Information and Security Review; and

xi. certain defense services and related unclassified technical data disclosed to nationals of NATO countries, Australia, Japan, and Sweden for purposes of responding to a written request from DoD for a quote or bid proposal.

B. The Export Administration Regulations

The Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, promulgated under the authority of the Export Administration Act ("EAA"), 50 U.S.C. App. §§ 2401-2420, control the export of commodities which have both military and commercial applications (i.e. dual-use items) and which are strictly commercial items.\(^1\) The EAR subject controlled commodities to licensing requirements and proscribes other conduct related to export activities. The Department of Commerce ("DoC") administers the EAR through the Bureau of Industry and Security ("BIS").

1. What is Controlled under the EAR?

a. Items subject to the EAR are identified in the Commerce Control List ("CCL"). The CCL is divided into Export Classification Numbers ("ECCNs") which are a five-character code. There are ten (10) industry category groups on the CCL: (0) Nuclear Materials, Facilities and Equipment, and Miscellaneous; (1) Materials, Chemicals, “Microorganisms,” and Toxins; (2) Materials Processing; (3) Electronics Design, Development and Production; (4) Computers; (5) Telecommunications and Information Security; (6) Sensors; (7) Navigation and Avionics;

---

\(^1\) Although the EAA expired in 1994, the EAA and the EAR remain in effect through annual executive orders issued pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1706.

b. The threshold duty of an exporter under the EAR is to determine whether an article or technology, or technical data is “subject to the EAR.” The term “subject to the EAR” means those commodities, software, technology, and activities over which BIS exercises regulatory jurisdiction under the EAR. Items not on the CCL may also be “subject to the EAR.”

c. EAR controls derive from several U.S. policy interests, including:

i. National Security: to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or countries, and which would prove detrimental to the national security of the United States.

ii. Foreign Policy and Nonproliferation: to restrict the export of goods and technology where necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations.

Note: Under this policy, controls are implemented for nuclear, chemical and biological weapons and missile proliferation. For this reason, foreign policy concerns have been increasingly important in recent years.

iii. Short Supply: to restrict the export of goods where necessary to protect the domestic economy from excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand.

2. What is not Controlled under the EAR?

Certain items and technologies are not “subject to the EAR”, and these are set forth in Part 734 of the EAR. Most importantly for universities, EAR controls do not apply to publicly available software and technology that (a) have been or will be published; (b) arise from fundamental research; (c) are educational; or (d) are included in certain patent applications.

3. What is Fundamental Research under the EAR?

a. Like the ITAR, the EAR do not impose export controls on fundamental research, which means basic and applied research in science and engineering conducted by scientist, engineers, or students at a university, where the resulting information is
ordinarily published and shared broadly within the scientific community. However, the fundamental research exemption does not apply to research the results of which are (a) subject to publication restrictions imposed by a sponsor, (b) subject to substantial prepublication review by a sponsor, or (c) subject to the sponsor withholding results from publication. Likewise, research resulting from U.S. Government-sponsored projects which are subject to specific national security controls are not considered fundamental and are subject to EAR controls. EAR §§ 734.8-11.

b. Similar to the ITAR fundamental research exemption, information released to a university by a third party, such as a government or commercial sponsor, is not within the EAR fundamental research exemption because it does not arise during or as the result of fundamental research.

c. Moreover, the fundamental research exemption under the EAR, like the ITAR, does not include research the results of which are subject to any restrictions placed on access or dissemination, whether as a result of proprietary rights restrictions or specific U.S. government controls. However, unlike the ITAR, the EAR fundamental research exemption allows prepublication review by sponsors solely to ensure that proprietary information is not inadvertently divulged and, so long as the review causes only a temporary delay in publication, to ensure that publication does not compromise patent rights.

4. **Who is a “Foreign Person” under the EAR?**

There is no definition of “foreign person” or “foreign national” contained in the EAR which applies comprehensively to that regime. Section § 746.5 of the EAR, which addresses special controls for exports to Iran, contains a definition of the term “foreign person” which is limited to that section of the EAR: “...the term ‘foreign person’ means those not defined as United States persons.” One may not unreasonably conclude that, despite the absence of an overall definition of the term, BIS would take the position, consistent with the guidance contained in EAR § 746.5, that a “foreign person” is someone who is not a “U.S. person”.

5. **Who is a “U.S. Person” under the EAR?**

The EAR contain several definitions of the term “U.S. person” for the purposes of regulating the export of dual-use products, technologies and information.
a. In the context of license requirements for the export of dual-use items, Parts 744 and 772 have identical definitions of the term “U.S. person” which include the following:

i. any individual who is a citizen of the United States, a permanent resident alien of the United States, or a protected individual as defined by 8 U.S.C. 1324b(a)(3);

ii. any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and

iii. any person in the United States.

b. EAR § 740.9, which authorizes a license exception for temporary imports, exports and reexports, contains a different definition, omitting the reference to “any person in the United States”;

c. EAR § 746.2, setting forth special country controls with respect to Cuba, defines “U.S. person” simply as “any person subject to the jurisdiction of the United States”, thereby incorporating a similar definition used by the Department of Treasury’s Office of Foreign Assets Control with respect to U.S. embargo requirements with respect to that country.

d. Similarly, EAR § 746.5, relating to special country controls for Iran, defines “U.S. person” to mean “any United States citizen, permanent resident alien, entity organized under the laws of the United States (including foreign branches), or any person in the United States...” As noted above, in perhaps the only attempt to define the term “foreign person”, EAR § 746.5 states that “...the term ‘foreign person’ means those not defined as United States persons.”

e. Finally, Part 760 of the EAR, which prescribes the antiboycott regulations discussed in more detail below, contains a very detailed definition of the term “U.S. person” and, also, some guidance as to who is not a “U.S. person”. The basic definition of “U.S. person”, as set forth in EAR § 760.1(b) includes “...any person who is a United States resident or national, including individuals, domestic concerns, and ‘controlled in fact’ foreign subsidiaries, affiliates, or other permanent foreign establishments of domestic concerns.”
6. What is an “Export” under the EAR?

a. EAR § 734 (b) contains a detailed explanation of the meaning of the term “export” under the EAR.

i. The basic definition of “export” is “...an actual shipment or transmission of items subject to the EAR out of the United States, or the release of technology or software subject to the EAR to a foreign national in the United States...” EAR § 734 (b)(1).

ii. The export of technology or software (other than encryption software subject to special “EI” controls) is further defined in EAR § 734 (b)(2) to include:

- any release of technology or software subject to the EAR in a foreign country; or

- any release of technology or source code subject to the EAR to a foreign national, which is “deemed to be an export to the home country or countries of the foreign national.” See discussion below concerning “deemed export” rule.

iii. Technology or software is considered to be “released” for export purposes, as set forth in EAR § 734 (b)(3), through:

- visual inspection by foreign nationals of U.S.-origin equipment and facilities;

- oral exchanges of information in the United States or abroad; or

- the application to situations abroad of personal knowledge or technical experience acquired in the United States.

iv. Encryption source code and object code software is considered to be exported when it is actually shipped, transferred, or transmitted out of the United States, or it is transferred in the United States to an embassy or affiliate of a foreign country. EAR § 734 (b)(9). However, the software is considered to be shipped, transferred or transmitted out of the United States by “downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or
making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code.” \textit{Id.}

v. Under the EAR § 734 (b)(5)&(6), a “reexport” means:

- an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country;

- the release of technology or software subject to the EAR to a foreign national outside the United States; or

- the release of technology or source code from one foreign national to a foreign national of another country.

7. EAR Requirements

a. Items on the CCL require export licenses unless license exceptions apply. License exceptions are pre-approved authorizations to export based on established criteria, all of which must be satisfied to use the exception.

b. If the commodity or technology is subject to the EAR, an exporter must establish whether any of the Ten (10) General Prohibitions apply to the export. These prohibitions require exporters to obtain a license unless the regulations state that a license exception overrides the license requirements. If one or more of the prohibitions applies, and no license exceptions may be used, then the exporter must seek a license from DoC. Only four of the General Prohibitions currently may be overcome by license exceptions.

c. General Prohibitions One (1) through Three (3) relate to product controls and can be used to exempt controlled products from the export license requirements:

\begin{align*}
\text{Prohibition One:} & \quad \text{Exports and Reexports} \\
\text{Prohibition Two:} & \quad \text{Parts and Components Reexports}
\end{align*}
Prohibition Three: Foreign-Produced Direct Product Reexports

d. General Prohibitions Four (4) through Ten (10) relate to activities that are prohibited without the express written permission of the BIS. Except for Prohibition Eight, these controls are not subject to license exceptions and, therefore, require export licenses in all circumstances:

Prohibition Four: Denial Orders
Prohibition Five: End-Use/End-User
Prohibition Six: Embargo
Prohibition Seven: U.S. Person Proliferation Activity
Prohibition Eight: Intransit
Prohibition Nine: Orders, Terms and Conditions
Prohibition Ten: Knowledge Violation [is] to Occur

e. Activities identified in Prohibitions 1-3 are subject to licensing and other requirements only to the extent one transfers items on the CCL. In contrast, EAR restrictions identified at Prohibitions 4-10 are general in nature and are not limited to exports of items on the CCL. They prohibit, for example, all exports under a denial order (Prohibition 4), those destined for embargoed destinations (Prohibition 6), and exports that support certain proliferation activities (Prohibition 7).

8. Exceptions to EAR Requirements

Part 740 of the EAR sets forth various License Exceptions, which authorize exports or reexports under specific conditions when the item or technology would otherwise require a license under General Prohibitions One, Two, Three, or Eight as indicated under the applicable ECCNs in the CCL.

9. The Antiboycott Regulations

a. The EAR also prohibit participation in boycotts or restrictive trade practices that are not supported by the United States. The primary example of such a boycott is the boycott of Israel by various
countries. The regulations impose reporting requirements on entities who receive any requests by third parties to participate in such activities. Reports must be filed with BIS detailing the request received. Details must include the nature of the request, the entity or person requesting participation in boycotting activities, the type of documents in which the request was received, and the response, if any, provided by the company receiving the request. U.S. entities or persons subject to the jurisdiction of the United States may not actively or passively respond to any request to participate in boycotting activities. The regulations also require companies to maintain records related to antiboycott activities for a period of five (5) years. Violations of the antiboycott regulations are punishable by substantial civil penalties.

b. The antiboycott regulations identify specific actions which U.S. persons subject to U.S. jurisdiction may not pursue. No licenses may be obtained to participate in any of the prohibited activities. The regulations specifically prohibit:

i. agreements to refuse or actual refusals to do business with or in a boycotted or blacklisted country or with nationals or residents of a boycotted country;

ii. agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality;

iii. agreements to furnish or actually furnishing information about business relationships with or in boycotted countries or blacklisted companies;

iv. agreements to furnish or the actual furnishing of information about the race, religion, sex, or national origin of another person;

v. agreements to furnish or the actual furnishing of information about business relationships with blacklisted companies or with blacklisted persons;

vi. agreements to furnish or the actual furnishing of information about associations with charitable and fraternal organizations; and

vii. implementing letters of credit containing prohibited boycott terms or conditions.
c. Inquiries or other activities related to these prohibitions may arise in numerous situations, and may seem innocuous. For example, requests could occur during negotiations, in contract language, under letters of credit, in financial arrangements, and in a foreign country’s import documentation. *No matter how or when the issue arises, responding to such requests, or agreeing to further the proscribed boycotting activities, is strictly prohibited.*

7. **Multilateral International Controls**

The U.S. Government participates in international export control regimes which impose specific responsibilities on exporters of U.S.-origin goods and technology. These international obligations are incorporated into the EAR in Part 742.

a. The Wassenaar Arrangement

i. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (the “Wassenaar Arrangement”) is the successor to the Coordinating Committee on Multilateral Export Controls (“COCOM”). The Wassenaar Arrangement requires members to obtain international approvals for specified, primarily dual-use items and technology. These items are normally governed by the DoC under the EAA and EAR.

ii. The current Wassenaar Arrangement members include: Argentina, Australia, Belgium, Bulgaria, Canada, The Czech Republic, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Spain, South Korea, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, and the United States.

iii. Since one of the stated purposes of the Wassenaar Arrangement is to complement and reinforce, but not duplicate, members’ existing control regimes, extensive additional licensing obligations are not anticipated, although the Arrangement may create additional recordkeeping and reporting requirements.

b. Missile Technology Control Regime (“MTCR”)

i. The Missile Technology Control Regime (“MTCR”) was established in 1987 to control proliferation of missile delivery systems which can be used for nuclear, chemical,
and biological weapons. The following countries are
signatories to the MTCR: Argentina, Australia, Austria,
Belgium, Brazil, Canada, Denmark, Finland, France,
Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan,
Luxembourg, the Netherlands, New Zealand, Norway,
Portugal, Russia, South Africa, Spain, Sweden,
Switzerland, the United Kingdom, and the United States.

ii. The term “missile” as used in these proliferation controls
means rocket systems (including ballistic missile systems,
space launch vehicles, and sounding rockets) and
unmanned air vehicle systems (including cruise missile
systems, target drones, and reconnaissance drones), capable
of delivering a payload to a range of at least 300 kilometers
(KM).

iii. Items controlled under the MTCR are divided into
Category I, Systems and Subsystems and Category II,
Other Components. U.S. regulations implementing the
MTCR are divided between the EAR and the ITAR.

c. Australia Group

The Australia Group is an international organization which has
established multilateral controls over chemical precursors,
chemical precursor production equipment, biological processing
equipment and related technical data. The membership of the
Australia Group includes: Argentina, Australia, Austria, Belgium,
Canada, The Czech Republic, Denmark, Finland, France,
Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan,
Luxembourg, the Netherlands, New Zealand, Norway, Poland,
Portugal, Romania, Slovakia, Spain, South Korea, Sweden,
Switzerland, the United Kingdom and the United States.

d. The Nuclear Suppliers Group

i. Nuclear proliferation is multilaterally controlled by the
Nuclear Suppliers Group (“NSG”). The NSG coordinates
multilateral export controls on dual-use items having
applications in nuclear weapons design and development,
and is comprised of the following countries: Argentina,
Australia, Austria, Belgium, Bulgaria, Canada, the Czech
Republic, Denmark, Finland, France, Germany, Greece,
Hungary, Ireland, Italy, Japan, Luxembourg, the
Netherlands, New Zealand, Norway, Poland, Portugal,
Romania, Russia, Slovakia, Spain, South Africa, Sweden,
Switzerland, the United Kingdom, and the United States.
ii. In the United States, nuclear-related, dual-use controls are implemented by Section 309 of the Nuclear Non-Proliferation Act, which requires the President to publish procedures for the DoC to control nuclear-related dual-use items.

C. The Foreign Assets Control Regulations


1. What is Controlled under the OFAC Regulations?

a. Under the OFAC-administered embargoes and sanctions, “U.S. persons” are generally prohibited from transacting business with identified narcotics traffickers, terrorist organizations, specially designated nations, or designated embargoed foreign countries, such as Burma, Cuba, Iran, and North Korea. The sanctions range from partial to full trade embargoes and are imposed in addition to other U. S. export control law penalties.

b. The regulations define prohibited transactions with foreign countries and set forth sanctions for engaging in such conduct. In this context, a transaction involves “any payment or transfer to any such designated foreign country or national, . . . any export or withdrawal from the United States to such designated foreign country, . . . and any transfer of credit, or payment of an obligation, expressed in terms of the currency of such designated foreign country.” The regulations state that a person subject to U.S. jurisdiction may not participate in:

i. transactions involving designated foreign countries or their nationals;

ii. transactions with respect to securities registered or inscribed in the name of a designated national;

iii. importation of and dealings in certain merchandise; and

iv. holding certain types of blocked property in interest-bearing accounts.

c. Persons subject to U.S. jurisdiction are also prohibited from dealing with specific entities or individuals known as “specially
designated nationals,” found in the Specially Designated Nationals List (“SDNL”), appended to the OFAC regulations. No one subject to U.S. jurisdiction may participate in any activity with anyone on the SDNL.

d. The regulations also allow for “blocking” or “freezing” assets of designated nationals. The term “blocking” or “freezing” is used to describe a form of controlling assets under U.S. jurisdiction. While title to blocked property remains with the designated country or national, the exercise of the powers and privileges normally associated with ownership is prohibited without authorization from OFAC. Blocking immediately imposes an across-the-board prohibition against transfers or transactions of any kind with regard to any property. Anyone subject to the regulations may not be involved with any account payments, transfers, withdrawals, or other dealings with those accounts unless such action is authorized by an OFAC license. U.S. individuals or organizations who violate the regulations by transacting business with designated nationals, specially designated nationals, or blocked accounts, may be subject to civil penalties or criminal prosecution.

e. OFAC regulations also define the type of property that is subject to control. Property is broadly defined to include: money, checks, drafts, debts, indebtedness, obligations, notes, warehouse receipts, bills of sale, negotiable instruments, contracts, goods, wares, merchandise, ships, goods on ships, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

2. Who is Subject to OFAC Regulations?

OFAC regulations apply to all persons subject to U.S. jurisdiction. This includes American citizens and permanent resident aliens wherever they are located; any individual or entity located in the U.S.; corporations organized under U.S. laws, including foreign branches; and, entities owned or controlled by any of the above, the most important being foreign-organized subsidiaries of U.S. corporations.

3. Requirements under the OFAC Regulations

a. U.S. persons must obtain licenses before they may engage in activities prohibited by the OFAC regulations. In limited cases, OFAC will provide general and special licenses to permit a U.S. person to engage in otherwise prohibited activities. The regulations provide for “general licenses,” which are similar to the License Exceptions of the EAR. Specific licenses, which are
permits issued by OFAC on a case-by-case basis, authorize particular individuals or entities to participate in an activity that would otherwise be prohibited by the embargo or sanctions programs. Specific licenses are granted sparingly and, if granted, are valid only for the specific activity proposed on the application.

b. The OFAC regulations impose both civil and criminal penalties for violations of TWEA, the IEEPA, and the regulations. Criminal convictions include prison sentences ranging from five (5) to twelve (12) years and fines which could exceed $250,000 for individuals and $1,000,000 for organizations. OFAC has independent authority to impose civil penalties for violations.

D. A Word about the Screening Lists

Whether controlled by DoC or DoS, an export otherwise permissible under the ITAR or the EAR may be prohibited because of the particular destination, end-use, or end-user. In addition to the OFAC-designated countries subject to embargo or sanction, the U.S. Government maintains a series of lists and publishes notices of persons, entities, and activities for which exports are strictly prohibited, or otherwise restricted. Universities, like all U.S. persons and entities, must institutionalize the screening of employees, contractors and subcontractors against these lists prior to transferring technical data, technology or services, whether domestically or overseas.

1. Denied Persons List

The denial or limitation of the privilege of exporting is one of many sanctions authorized under U.S. export laws and regulations. Parties denied exporting privileges by DoC are generally precluded from participating in any manner in any export-related transaction subject to the EAR. Sanctions can be imposed for engaging in export transactions with such “Denied Parties”. United States exporters must therefore ensure that all parties to their export transactions (including freight forwarders, intermediate consignees, end-users, and others are not on the Table of Denial orders). A list is published by DoC of persons who have been denied export privileges, in whole or in part. (See Supplement No. 2 of Part 764 of the EAR). Most transactions, including exports to, exports for, reexports, and intra-country transfers abroad, with denied persons are prohibited without prior authorization from the U.S. Government.

2. Specially Designated Nationals List
As noted above, OFAC publishes the SDNL, a list of specially designated persons and entities with whom any transactions are restricted. Exports to persons or entities on the list may not be conducted without prior authorization from OFAC.

3. **Debarred and Suspended Parties Lists**

DoS publishes in the Federal Register a list of parties whose export privileges have been revoked or suspended. Exports to these parties are prohibited. In rare circumstances, DoS may authorize an export to a debarred or suspended party when it is in the national interest.

4. **Proscribed Missile Technology Lists**

DoC prohibits the export or reexport to any destination without a license of items subject to the EAR, if the exporter knows or has reason to know that the export is destined for specific missile projects, or will be used in the design, development, production or use of missiles in or by certain countries. DoS may also control certain missile-related items that are concurrently found on the Commerce Control List. Prior approval may be required from both DoS and DoC prior to the export of these items. The EAR contains a list of missile-related facilities and technologies controlled for these purposes.

5. **Proscribed Chemical and Biological Weapons List**

DoC maintains a list of chemical and biological weapons (“CBW”), end-uses, and end-users, for which the export of any item subject to the EAR requires a license, including items for which no license is required. Exports for the designated end-uses and end-users may not be conducted without prior authorization from DoC.

6. **Proscribed Destination Restrictions/Entities List**

Exports to destinations or entities under sanctions are strictly controlled. DoC and DoS publish lists of destinations and entities sanctioned pursuant to United States law. Recent examples have included sanctions against India and Pakistan. Exports of defense articles and defense services to listed destinations are strictly prohibited.

E. **The Role of U.S. Security Clearance Regulations**

Research universities performing work on DoD contracts or other contracts related to national defense, security or intelligence programs may be subject to U.S. security clearance regulations which limit, if not totally prohibit, the involvement of foreign persons. These security regulations are independent of ITAR and EAR requirements.
   a. DoD, in conjunction with the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency, promulgated the National Industrial Security Program Operating Manual (“NISPOM”), DoC 5220.22-M, pursuant to the National Industrial Security Program (“NISP”) established by Executive Order 12829. The NISPOM provides industry standards and regulations for the safeguarding, use, and marking of classified information.

   b. Under the NISPOM, only U.S. citizens are eligible for security clearances unless there is some compelling reason to grant such access. NISPOM § 2-210. In the rare circumstances permitting access by a non-U.S. citizen to classified material, a Limited Access Authorization (“LAA”) may be granted. Id. The burden of certification of citizenship for personal security clearances is on the contractor. NISPOM § 2-206. Acceptable proof of citizenship includes birth certificates, naturalization certificates, passports and certain military identifications. NISPOM § 2-207.

   c. The NISPOM contains specific provisions regarding U.S. Government policy and procedures governing the control of classified information in international programs. NISPOM Chapter 10.

2. DoD Regulations
   a. Similar to the NISPOM requirements, DoD has its own internal regulations pertaining to classified information. The DoD Personnel Security Program regulations apply to all DoD civilian and military personnel, as well as contractor personnel affiliated with DoD. 32. C.F.R. § 154.2.

   b. Under the personnel security regulations, only U.S. citizens are eligible for security clearances or assignment to sensitive duties, or are otherwise granted access to classified information. 32 C.F.R. §154.6 As under the NISPOM, special circumstances may require the issuance of an LAA to otherwise grant access to non-U.S. citizens. Id.

F. Homeland Security and the Government Technology Alert List
Legislation such as the Patriot Act, passed in the wake of September 11, and the accompanying reorganization of the federal government resulting in the new Homeland Security Department, did not change the content of U.S. export control laws and regulations nor the organization of export enforcement authorities. However, brief mention will be made here of the Technology Alert List ("TAL") which is being used by the U.S. Government effectively as a control on the disclosure of certain technologies to foreign persons – independently of conventional export control regimes.

1. The TAL is a list containing sensitive goods, technology or information whose export is prohibited. Among the fields covered by the TAL are:
   a. information security: technologies associated with cryptography to ensure secrecy for communications, video data and related software;
   b. robotics and artificial intelligence: automation, machine tools, pattern recognition technologies;
   c. advanced computer/microelectronic technology: supercomputing, hybrid computing, speech processing/recognition systems, neural networks, data fusion, frequency synthesizers, etc.;
   d. navigation, avionics and flight control: internal navigation systems, flight control systems, even Global Positioning Systems (GPS);
   e. sensors and sensor technology: marine acoustics, optical sensors, night vision devices, image intensification devices, high speed photographic equipment;
   f. other fields: biomedical engineering, laser systems, marine, nuclear engineering.

2. The TAL can be used by visa officers in consular offices worldwide as a basis on which to deny visas to particular visa applicants, if the officer believes the applicant will gain access in the United States to goods, technology or sensitive information whose export is prohibited. The TAL can be used as a basis on which to deny visas to any foreign person – from ally countries and trading partners as well as "suspect" countries.

3. The visa officer’s “belief” that an unlawful technology transfer will occur is sufficient to deny the visa. As a result, a foreign Ph.D. or Senior Researcher whose purpose for visiting the United States includes involvement in programs or activities within the fields encompassed by the TAL will be subject to visa interviews and questioning about her or his research and its uses. A visa officer who is unsatisfied by answers given
during the interview will refer the matter to the DoS in Washington for resolution of the security issues. Until resolved favorably to the visa applicant, no visa will issue.

III. THE “DEEMED EXPORT” RULE

A. When does a “Deemed Export” Arise?

1. The so-called “deemed export” rule is applied under both the EAR and the ITAR. Under the EAR, “[a]ny release of technology or source code subject to the EAR to a foreign national …is deemed to be an export to the home country or countries of the foreign national.” EAR § 734.2(b)(2)(ii). Under the ITAR, an “[e]xport [includes]…[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person [or]…[p]erforming a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.” ITAR § 120.17(4).

2. However, the ITAR, unlike the EAR, permit disclosures of unclassified technical data in the U.S. by U.S. institutions of higher learning to foreign persons who are their bona fide and full-time regular employees, with certain conditions. ITAR § 125.4(b)(9).

B. Who is a “Foreign Person”?

1. The ITAR use the term “foreign person” to mean “[a]ny natural person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3).” ITAR § 120.16.

2. The EAR do not directly define either “foreign national” or “foreign person”. But, instructively, the EAR provide that the “…deemed export rule does not apply to persons lawfully admitted for permanent residence in the United States and does not apply to persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).” EAR § 734.2(b)(2)(ii). The policy of the BIS in implementing the EAR is to view the last-acquired citizenship or permanent residency as the determinant of home country for deemed export purposes. But, knowledge or reason to know that a diversion of technology will occur to a country other than the presumed home country obligates the exporter to inquire further, seek a license based on likely diversion, or cease the transaction.

C. The Challenges of Technical Data Exports and the “Deemed Export” Rule
1. The “deemed export” rule is controversial, because it is at once an impediment to free exchange of information and ideas, and a barrier to the recruitment of skilled professionals. The scope of the “deemed export” rule should not be underestimated. The rule covers virtually any means of communication with a foreign national, whether face-to-face; via telephone, e-mail or fax; through the sharing of computer files; and, during visual inspections or site tours. The rule also includes “reexports”, i.e. communications with a foreign national abroad involving the disclosure of U.S.-origin technology legally exported originally.

2. Moreover, the “deemed export” rule arises in the context of exports of technology, technical data, information and software (“technical data”). The transfer of technical data is often perceived as intangible and therefore not subject to export controls. Contrary to this perception, technical data are controlled just as other commodities and products, warranting attention to special areas of concern regarding transfer of technical data to foreign national researchers, contractors and visitors.

3. Technical data must be handled similarly to other commodities and products controlled on the CCL and the USML. Any release of technical data related to items controlled by the CCL or the USML to a foreign national is considered an export. Thus, the release of technical data may require a license or approval prior to export, or if a transfer - as with a product - would otherwise be subject to special restrictions under the regulations (e.g., transfers to proscribed destinations and end-users, embargoed countries, denied parties).

4. Under both the EAR and the ITAR, technical data includes:

   a. technology, or information required to design, develop, produce, manufacture, assemble, operate, repair, maintain, modify or test controlled items;

   b. blueprints, drawings, photographs, plans, instructions and other documentation relating to controlled items;

   c. classified information relating to dual-use items or defense articles, services;

   d. software; and

   e. technical assistance, including instruction, skills building, training, and working knowledge relating to controlled items.

5. Under both the EAR and the ITAR, technical data typically does not include:
a. general scientific, mathematical or engineering principles; and

b. basic marketing information regarding function or purpose or
general system descriptions of defense articles or dual-use goods
or technology;

c. information in the public domain; or

d. standard facility tours offered to the general public.

6. Technical data and its management for export compliance purposes
represents an area of special concern because of the varied and intangible
ways of transferring information. Exports of controlled technical data can
occur when information is sent or taken abroad in any form, or when
information is disclosed or transferred to a foreign national whether in the
United States or abroad (i.e. the “deemed export”). Examples of possible
export scenarios include:

a. conversations or meetings with a foreign researcher, graduate
   student, or others in the university community;

b. visual inspection of U.S.- origin equipment and facilities by
   foreign nationals;

c. presentations at conferences;

d. submission of articles for outside publication;

e. brochures and displays;

f. placing controlled information on the internet;

g. exchanges by e-mail or fax to foreign destinations or individuals;
or

h. utilization of express mail or other services (e.g., DHL, Federal
   Express);

D. Pay Particular Attention to the Internet

DoS and DoC have determined that placing data onto the Internet is an export and
must be treated as such. The “publishing” of data on the Internet is treated in the
same manner as the publishing of data in any other forum. The data must fall into
one of the following criteria prior to publication or release:

1. The data is “Public Domain” as defined in §120.11 of the
   ITAR, or is “Publicly Available” under Part 772 of the
   EAR.

   National Association Of College and University Attorneys

   28
2. Pursuant to §125.4(b)(13) of the ITAR the data has been cleared for release by either the Directorate for Freedom of Information and Security Review (DFOISR) or the Cognizant U.S. Government Department or Agency.

3. Necessary export approvals have been obtained. However, obtaining an export license for controlled technical data to be released over the Internet is most unlikely. Data placed onto the Internet is available around the world and a license is unlikely to be approved for such a broad end-user base.