THE UNIVERSITY OF ALABAMA
AT BIRMINGHAM

EXPORT COMPLIANCE PROGRAM MANUAL

List of Abbreviations

D:OSP	Director in Office of Sponsored Programs
BIS	Department of Commerce Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
DDTC	Department of State Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
UCO	University Export Controls Officer
ITAR	International Traffic in Arms Regulations
OFAC	Department of the Treasury Office of Foreign Assets Control
OSP	Office of Sponsored Programs
PI	Principal Investigator
SDN List	Specially Designated Nationals and Blocked Persons List
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List
UAB	The University of Alabama at Birmingham

Table of Contents

OVERVIEW OF EXPORT CONTROLS

I. INTRODUCTION

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

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

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

II. EXPORT CONTROLS AND UNIVERSITY RESEARCH

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

Export controls present unique challenges to universities and colleges because they require balancing concerns about national security and U.S. Economic vitality with traditional concepts of unrestricted academic freedom, and publication and dissemination of research

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

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

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

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

A. ITEMS CONTROLLED UNDER THE ITAR

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

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

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

---

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

[3] 22 C.F.R. § 120.6.

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

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

B. THE USML CATEGORIES

The USML designates particular categories and types of equipment as defense articles and associated technical data and defense services.[6] The USML divides defense items into 21 categories, listed below. An electronic version of the USML is available on the Department of State website at: http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf.

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

C. CLASSIFICATION

While DDTC has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify the item. If doubt exists as to whether an

[5] 22 C.F.R. § 120.9.

[6] *See* 22 C.F.R. § 121.1.

article or service is covered by the USML, upon written request in the form of a Commodity Jurisdiction ("CJ") request, DDTC will provide advice as to whether a particular article is a defense article subject to the ITAR, or a dual-use item subject to Commerce Department licensing.[7] Determinations are based on the origin of the technology (*i.e.*, as a civil or military article), and whether it is predominantly used in civil or military applications. University employees should contact the University Compliance Office ("UCO") when classifying an item. If the University of Alabama at Birmingham ("UAB") needs to obtain a CJ determination, the UCO will file the CJ request with DDTC.[8]

D. DEFINITION OF EXPORT UNDER THE ITAR

The ITAR defines the term "export" broadly. The term applies not only to exports of tangible items from the U.S., but also to transfers of intangibles, such as technology or information. The ITAR defines as an "export" the passing of information or technology to foreign nationals even in the United States."[9] The following are examples of exports:

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

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

2. Extra-territorial transfers

- The re-export or re-transfer of defense articles from one foreign person to another, not previously authorized (*i.e.*, transferring an article that has been exported to a foreign country from that country to a third country).
- Transferring the registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether the transfer occurs in the United States or abroad.

3. Export of intangibles

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

---

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

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

[9] 22 C.F.R. § 120.17.

E. AUTHORIZATION TO EXPORT

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

However, university researchers are usually engaged only in the creation of unclassified technical data, or engaged only in the fabrication of articles for experimental or scientific purpose, including research and development. Therefore, the university is not usually required to register with DDTC. [12]

However, if the university desires to involve foreign nationals in ITAR-controlled research, it must register with the DDTC to apply for a license or take advantage of certain license exemptions. License exemptions specific to universities, as well as licensing procedures, are described in detail in the *Key Issues in University Research* section, below.

F. EMBARGOED COUNTRIES UNDER DDTC REGULATIONS

ITAR Prohibitions. In general, no ITAR exports may be made either under license or license exemption to countries proscribed in 22 C.F.R. § 126.1, such as China, Cuba, Iran, North Korea, Sudan, and Syria. Additional restrictions apply to other countries; a complete list of U.S. arms embargoes is available online at: http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf.

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

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

---

[10] 22 C.F.R. § 122.1.

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

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

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

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

A. ITEMS CONTROLLED UNDER THE EAR

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

The EAR requires a license for the exportation of a wide range of items with potential "dual" commercial and military use, or otherwise of strategic value to the United States (but not made to military specifications). However, only items listed on the *Commerce Control List* ("CCL") require a license prior to exportation. Items not listed on the CCL are designated as EAR99 items and generally can be exported without a license, unless the export is to an embargoed country, or to a prohibited person or end-use.[14] The following summarizes the types of items controlled under the EAR:

- **Commodities**. Finished or unfinished goods ranging from high-end microprocessors to airplanes, to ball bearings.

- **Manufacturing Equipment**. This includes equipment specifically for manufacturing or testing controlled commodities, as well as certain generic machines, such as computer numerically controlled ("CNC") manufacturing and test equipment.

- **Materials**. This includes certain alloys and chemical compounds.

- **Software**. This includes software specifically associated with particular commodities or manufacturing equipment, as well as any software containing encryption and the applicable source code.

- **Technology**. Technology, as defined in the EAR, includes both technical data, and services. Unlike the ITAR, there is generally no distinction between the two. However, the EAR may apply different standards to technology for "use" of a product than for the technology for the "design" or "manufacture" of the product.

106-508 (114 Stat. 2360 (2000)) and it remained in effect through August 20, 2001. Since August 21, 2001, the Act has been in lapse and the President, through Executive Order 13222 of August 17, 2001, which has been extended by successive Presidential Notices, has continued the EAR in effect under IEEPA.

[14] 15 C.F.R. § 734.

B. THE COMMERCE CONTROL LIST CATEGORIES

The CCL provides a list of very specific items that are controlled. The CCL is similar to the "dual-use" list adopted by other countries under the Wassenaar Arrangement,[15] although the CCL has additional items. The CCL is divided into the nine categories below. The CCL is available online at http://www.access.gpo.gov/bis/ear/ear_data.html.

CATEGORIES

0.		Nuclear related items & miscellaneous items
1.		Chemical compounds, microorganisms and toxins
2.		Materials processing
3.		Electronics
4.		Computers
5.	pt-1	Telecommunications
5.	pt-2	Information security (encryption)
6.		Sensors & lasers
7.		Navigation and avionics
8.		Marine (vessels, propulsion, and equipment)
9.		Propulsion systems, space vehicles (includes aircraft & aircraft engines)

C. CLASSIFICATION

As discussed in *Overview*, Section III.C, DDTC has jurisdiction to decide whether an item is ITAR- or EAR-controlled. DDTC encourages exporters to self-classify the product. If doubt exists, a CJ request may be submitted to DDTC to determine whether an item is ITAR- or EAR- controlled.[16]

Once it is determined that an item is EAR-controlled, the exporter must determine its Export Control Classification Number ("ECCN"). The BIS has two assistance procedures where the proper ECCN classification or licensing requirements are uncertain.[17] To determine EAR's applicability and the appropriate ECCN for a particular item, a party can submit a "Classification Request" to BIS. To determine whether a license is required or would be granted for a particular transaction, a party can request BIS provide a non-binding "advisory opinion." While BIS provides assistance with determining the specific ECCN of a dual-use item listed on the CCL, if doubt exists as to whether an item is ITAR- or EAR-controlled, BIS will stay its classification proceeding and forward the issue to DDTC for jurisdiction determination.

---

[15] Information on the Wassenaar Arrangement is available at: http://www.bis.doc.gov/wassenaar/default.htm.

[16] For a complete discussion, *see Overview of Export Controls*, Section III.C above.

[17] *See* 15 C.F.R. § 748.3.

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

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

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

2. Deemed Export. Under the EAR the release of technology to a foreign national in the United States is "deemed" to be an export, even though the release took place within the United States. Deemed exports may occur through such means as a demonstration, oral briefing, or plant visit, as well as the electronic transmission of non-public data that will be received abroad.

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

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

E. AUTHORIZATION TO EXPORT

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

The EAR contains a number of exceptions. Determining whether a particular exception applies requires review of the specific application as detailed in 15 C.F.R. § 740, as well as review of the notes on applicable license exceptions following the ECCN entry on the CCL.[18]

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

[18] 15 C.F.R. § 740.

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

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

AT	Anti-Terrorism	CB	Chemical & Biological Weapons
CC	Crime Control	CW	Chemical Weapons Convention
EI	Encryption Items	FC	Firearms Convention
MT	Missile Technology	NS	National Security
NP	Nuclear Nonproliferation	RS	Regional Security
SS	Short Supply	XP	Computers
SI	Significant Items		

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

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

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

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

LVS	Items of limited value (value is set under each ECCN).
GBS	Items controlled for national security reasons to Group B countries.
CIV	Items controlled for national security reasons to particular countries where end-user is civilian.
TSR	Certain technology and software to certain countries.
APP	Computer exports to certain countries.

KMI	Encryption exemption for key management.
TMP	Certain temporary exports, re-exports, or imports, including items moving through the U.S. in transit.
RPL	Certain repair and replacement parts for items already exported.
GFT	Certain gifts and humanitarian donations.
GOV	Exports to certain government entities.
TSU	Certain mass-market technology and software.
BAG	Baggage exception.
AVS	Aircraft and vessels stopping in the U.S. and most exports of spare parts associated with aircraft and vessels.
APR	Allows re-export from certain countries.
ENC	Certain encryption devices and software.
AGR	Agricultural commodities.
CCD	Authorization of certain consumer communication devices to Cuba.

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

V. OFAC SANCTIONS PROGRAM AND BARRED ENTITIES LISTS

A. SANCTIONED COUNTRIES

U.S. Economic sanctions broadly prohibit most transactions between a U.S. person and persons or entities in an embargoed country, including Cuba, Iran, North Korea, Syria, and Sudan.[19] This prohibition includes importation and exportation of goods and services, whether direct or indirect, as well as "facilitation" by a U.S. person of transactions between foreign parties and a sanctioned country. For example, sending a check to an individual in Iran could require an OFAC license or be prohibited. More limited sanctions may block particular transactions or require licenses under certain circumstances for exports to a number of countries,

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

including but not limited to Burma, Liberia, and Zimbabwe.[20] Because this list is not complete and subject to change, please visit http://www.treas.gov/offices/enforcement/ofac/.

While most sanctions are administered by OFAC, BIS has jurisdiction over certain exports prohibitions (via "embargo" regulations), as is the case with exports to Syria.[21] In other words, a license from BIS would be required to ship most items to Syria and other OFAC sanctioned countries or could be prohibited. Economic sanctions and embargo programs are country-specific and very detailed in the specific prohibitions.

B. TERRORIST AND OTHER BARRED ENTITY LISTS

Various U.S. Government agencies maintain a number of lists of individuals or entities barred or otherwise restricted from entering into certain types of transactions with U.S. persons. Particularly since 9/11, U.S. companies are beginning to become more assertive in attempting to place contractual terms with foreign companies related to these lists. Such lists must be screened to ensure that the university does not engage in a transaction with a barred entity. UAB, under a UT system-wide license, uses Visual Compliance™ to expedite screening of these and other lists.

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

- **Persons Named in General Orders (15 C.F.R. § 736, Supp. No. 1).** General Order No. 2 contains the provisions of the U.S. embargo on Syria; General Order No. 3 prohibits the re-exports to Mayrow General Trading and related parties. A link to the General Orders is available at: http://www.access.gpo.gov/bis/ear/pdf/736.pdf.

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

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

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

---

[20] *See* http://www.treas.gov/offices/enforcement/ofac/ for a full list of U.S. sanction programs.

[21] *See* 15 C.F.R. § 746.

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

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

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

VI. ANTI-BOYCOTT RESTRICTIONS

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

Anti-boycott restrictions are most likely to appear in dealings with entities in certain Arab League countries. As of this writing, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and Yemen continue to impose boycott restrictions on Israel and companies that do business with Israel. Iraq is not included in this list, but its status with respect to the future lists remains under review by the Department of Treasury.[22] Egypt and Jordan have ceased participating in the boycott.

Note that there are strict reporting requirements even where the U.S. person refuses to participate in a requested boycott action.

A. JURISDICTION

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

- A foreign company's affiliate or permanent office in the U.S.

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

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

B. RED FLAGS

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

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

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

C. EXCEPTION

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

D. REPORTING

Any U.S. person or entity who is asked to enter into an agreement or provide information that would violate anti-boycott laws must report this to BIS using a form BIS-621-P in accordance with 15 C.F.R. § 760.5. Information regarding the reporting of suspected anti-boycott activities can be found at:
http://www.bis.doc.gov/ComplianceAndEnforcement/index.htm.
In addition, the U.S. Internal Revenue Service (IRS) requires U.S. taxpayers to report operations in or relating to boycotting countries and nationals and request to cooperate with boycott activities. *See* IRS Form 5713, located online at: http://www.irs.gov/pub/irs-pdf/f5713.pdf.

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

For more information on anti-boycott rules see:
http://www.bis.doc.gov/complianceandenforcement/antiboycottcompliance.htm. The Office of

Boycott Compliance has also set up an advice line for questions about the anti-boycott rules, which can be reached at (202) 482-2381.

VII. PENALTIES FOR EXPORT VIOLATIONS

A. GENERAL OVERVIEW

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

B. DEFENSE EXPORTS

The Arms Export Controls Act and the ITAR provide that wilful violations of the defense controls can be fined up to $1,000,000 per violation, or ten years of imprisonment, or both.[23] In addition, the Secretary of State may assess civil penalties, which may not exceed $500,000 per violation.[24] The civil penalties may be imposed either in addition to, or in lieu of, any other liability or penalty. The articles exported or imported in violation, and any vessel, vehicle or aircraft involved in such attempt is subject to seizure, forfeiture and disposition.[25] Finally, the Assistant Secretary for Political-Military Affairs may order debarment of the violator, *i.e.*, prohibit the violator from participating in export of defense items.[26]

While imposing criminal liability is fairly rare, many major U.S. companies have been assessed significant civil penalties in the millions of dollars.[27] For example, an investigation into the export practices of ITT Corporation, the leading manufacturer of military night vision equipment for the U.S. Armed Forces, resulted in the company's Night Vision Division being debarred from export of defense items for three years. In addition, pursuant to a plea agreement ITT agreed to pay a total of $100 million for its violations of defense export laws, one of the largest penalties ever paid in a criminal or civil case.[28]

---

[23] 22 U.S.C. § 2778(c) and 22 C.F.R. § 127.3.

[24] 22 U.S.C. § 2778(e) and 22 C.F.R. § 127.10.

[25] 22 C.F.R. § 127.6.

[26] 22 U.S.C. § 2778(g) and 22 C.F.R. § 127.7.

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

[28] *See* Bureau of Political-Military Affairs; Statutory Debarment of ITT Corporation Pursuant to the Arms Export Control Act and the International Traffic in Arms Regulations, 72 Fed. Reg. 18310 (Apr. 11, 2007). For a detailed account of the ITT Corporation investigation, *see* the U.S. Department of Justice press release "ITT Corporation to Pay $100 Million Penalty and Plead Guilty to Illegally Exporting Secret

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

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

Similarly to the ITAR, violations of the EAR are subject to both criminal and administrative penalties. Fines for export violations, including anti-boycott violations, can reach up to $1,000,000 per violation in criminal cases, and $250,000 per violation in most administrative cases. In addition, criminal violators may be sentenced to prison time up to 20 years, and administrative penalties may include the denial of export privileges.[29] A denial order is probably the most serious sanction because such order would bar a U.S. company from exporting for a period of years or bar a foreign entity from buying U.S. origin products for such period.

In most instances, BIS reaches negotiated settlements in its administrative cases, as a result of voluntary self-disclosures of violations by companies and individuals. Voluntary disclosures constitute a major mitigating factor in determining penalties, reducing the amount of penalty by up to 50 percent, provided certain conditions are met, such as the implementing of a comprehensive compliance program.[30]

D. EXPORTS TO A SANCTIONED COUNTRY

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

---

Military Data Overseas" (March 27, 2007), available at: http://www.usdoj.gov/opa/pr/2007/March/07_nsd_192.html.

[29] These violations are based on the Export Administration Act of 1979, as amended (50 U.S.C. app. §§ 2401-2420), and inflation adjustments made in 15 C.F.R. § 6.4. From August 21, 1994, through November 12, 2000, the Act was in lapse. During that period, the President, through Executive Order 12924, which had been extended by successive Presidential Notices, continued the EAR in effect under the International Emergency Economic Powers Act (50 U.S.C. §§ 1701-1706 (IEEPA). On November 13, 2000, the Act was reauthorized by Pub. L. No. 106-508 (114 Stat. 2360 (2000)) and it remained in effect through August 20, 2001. Since August 21, 2001, the Act has been in lapse and the President, through Executive Order 13222 of August 17, 2001, which has been extended by successive Presidential Notices, has continued the EAR in effect under IEEPA. The USA PATRIOT Improvement and Reauthorization Act of 2005, signed into law on March 9, 2006 (Pub. L. No. 109-177, 120 Stat. 192 (2006)), increased the limit of civil penalties available under IEEPA to $50,000. On October 16, 2007, President Bush signed the International Emergency Economic Powers Enhancement Act, Pub. Law No. 110-96, which amends IEEPA by increasing civil penalties up to $250,000 per violation, and criminal penalties up to $1,000,000 per violation.

[30] For a review of BIS investigations and penalties, *see* "Don't Let This Happen to You! Actual Investigations of Export Control and Anti-boycott Violations" at http://www.bis.doc.gov/complianceandenforcement/dontletthishappentoyou-2008.pdf.

$250,000 per violation under OFAC regulations, with the exception of exports to Cuba.[31] Violations of the Cuban sanctions are subject to a maximum penalty of $65,000 per violation.[32]

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

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

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

[32] The OFAC embargo of Cuba was promulgated under the Trading with the Enemy Act (TWEA).

KEY ISSUES IN UNIVERSITY RESEARCH

I. DEEMED EXPORTS

While exports are commonly associated with the shipment of a tangible item across the U.S. border, export controls have a much broader application. One of the most difficult issues with respect to export controls is the fact that an export is defined to include the transfer of controlled *information or services* to foreign nationals even when the transfer takes place within the territory of the United States. Though taking place inside the U.S., the transfer is "deemed" to be an export (as if exporting to the country of the foreign national). The term "deemed export" is unique to the EAR.

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

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

The issue of deemed exports is particularly relevant to university research because of the activities that normally take place at a university. While a university may be involved in the shipment abroad of equipment or machinery to participate in a conference, a joint project, or equipment loan programs, most often faculty and students are engaged in teaching and research. Whenever teaching or research is related to controlled equipment or technology, foreign students' or researchers' involvement may trigger export control compliance issues.

II. U.S. AND FOREIGN PERSONS

For purposes of defense and dual-use exports, a *U.S. person* is defined as a U.S. entity or a U.S. citizen, a person lawfully admitted for permanent residence in the United States (*i.e.*, green card holder), or a person who is a protected individual under the Immigration and Naturalization Act (8 U.S.C. § 1324b(a)(3) (*i.e.*, certain classes of asylees).[33] A U.S. person may be engaged in activities that are export controlled, unless there are some additional restrictions that limit participation to U.S. citizens.

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

Note that the definitions for a U.S. and a foreign person differ for purposes of the OFAC sanctions. For a discussion, see *Overview of Export Controls*, Section V, above.

III. INFORMATION NOT SUBJECT TO OR EXCLUDED FROM EXPORT CONTROLS

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

A. PUBLICLY AVAILABLE

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

- **ITAR provision:** The ITAR describes such information as information in the *public domain*.[34] The information in the public domain may be obtained through:
    - sales at newsstands and bookstores;
    - subscription or purchase without restriction to any individual;
    - second class mailing privileges granted by the U.S. Government;
    - at libraries open to the public;
    - patents available at any patent office;
    - unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, **in the United States**;

[33] 22 C.F.R. § 120.15; 15 C.F.R § 734.2(b).

[34] 22 C.F.R. §§ 120.10(a)(5) and 120.11.

- public release in any form after approval of the cognizant U.S. Government agency; or

- *fundamental research* in the U.S. (*See Key Issues in University Research,* Section III.C. *Fundamental Research,* below.)

- **EAR provision:** The EAR does not control publicly available technology if it is already published or will be published.[35] Information is published when it becomes generally accessible to the interested public in any form, including:

  - publication in periodicals, books, print, *etc*., available for general distribution **free or at cost**;

  - readily available at libraries open to the public or university libraries;

  - patents and open patents applications available at any patent office; or

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

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

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

B. EDUCATIONAL INFORMATION

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

- **ITAR provision:** The ITAR specifically provides that the definition of "technical data" does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities.[36]

- **EAR provision:** The EAR provides that publicly available "educational information" is not subject to the EAR, if it is released by instruction in catalogue courses and associated teaching laboratories of academic institutions.[37]

[35] 15 C.F.R. §§ 734.3(b)(3) and 734.7.

[36] 22 C.F.R. § 120.10(a)(5).

[37] 15 C.F.R. §§ 734.3(b)(3) and 734.9.

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

The information will not be controlled even if the course contains recent and unpublished results from laboratory research, so long as the university did not accepted separate obligations with respect to publication or dissemination, *e.g.*, a publication restriction under a federal funding.[38]

C. FUNDAMENTAL RESEARCH

During the Reagan administration, several universities worked with the Federal government to establish national policy for controlling the flow of information produced in federally funded fundamental research at colleges, universities and laboratories resulting in the issuance of the National Security Decision Directive 189 ("NSDD"), National Policy on the Transfer of Scientific, Technical and Engineering Information on September 21, 1985. In a letter dated November 1, 2001, President George W. Bush's administration reaffirmed NSDD 189. NSDD 189 provided the following definition of *fundamental research* that has guided universities in making licensing decisions relative to fundamental research exclusions provided under both the EAR and ITAR.

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

Research conducted by scientists, engineers, or students at a university normally will be considered fundamental research. University based research is not considered *fundamental research* if the university or its researchers accept (at the request, for example, of an industrial sponsor) other restrictions on publication of scientific and technical information resulting from the project or activity. Scientific and technical information resulting from the research will nonetheless qualify as fundamental research once all such restrictions have expired or have been removed.

Both the ITAR and the EAR provide that information published and generally accessible to the public through fundamental research is not subject to export controls. However, there are certain restrictions. In order to take advantage of this exemption:

- such information must be produced as part of basic and applied research in science and engineering and must be broadly shared within the scientific

---

[38] 15 C.F.R. § 734, Supp. No. 1, Questions C(1) to C(6).

community (*i.e.*, no restrictions on publication / dissemination of the research results);[39]

- it is essential to distinguish the information or product that results from the fundamental research from the conduct that occurs within the context of the fundamental research;

- while the results of the fundamental research are not subject to export controls, an export license may be required if during the conduct of the research export controlled technology is to be released to a foreign national. Such export controlled technology may come from the research sponsor, from a research partner institution, or from a previous UAB research project.[40]

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

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

- **ITAR provision:** the fundamental research exception does not apply to research the results of which are restricted for proprietary reasons, or specific U.S. Government access and dissemination controls.[41]

- **EAR provision:** the fundamental research is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary reasons or specific national security reasons.[42] Under the EAR, university-based research is not considered fundamental research if the university or its researchers accept restrictions (other than review to ensure no release of sponsor-provided proprietary or patent information) on publication of scientific and technical information resulting from the project.[43]

The EAR instructs that prepublication review by a sponsor of university research solely to ensure that the publication would not inadvertently divulge proprietary information that the

---

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

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

[41] 22 C.F.R. §§ 120.11(a)(8) and 120.10(a)(5).

[42] EAR § 734.8(a).

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

sponsor has initially furnished, or compromise patent rights, does not constitute restriction on publication for proprietary reasons.

The EAR also has provided examples of "specific national security controls" which will trigger export controls. These include requirements for prepublication review and approval by the Government, with right to withhold permission for publication; restriction on prepublication dissemination of information to non-U.S. citizens or other categories of persons; or restrictions on participation of non-U.S. citizens or other categories of persons in the research.[44]

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

D. FULL-TIME UNIVERSITY EMPLOYEES

Under a specific exemption, the ITAR allows a university to disclose unclassified technical data in the U.S. to a foreign person who is the university's *bona fide* and full time regular employee. The exemption is available only if:

- the employee's permanent abode throughout the period of employment is in the United States;
- the employee is not a national of a country to which exports are prohibited pursuant to ITAR § 126.1 (See current list of countries at http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf);
- the university informs the individual in writing that the technical data may not be transferred to other foreign persons without the prior written approval of DDTC; and
- the university documents the disclosure of technical data under the exemption providing: (1) a description of the technical data; (2) the name of the recipient / end-user; (3) the date and time of export; (4) the method of transmission (*e.g.*, e-mail, fax, FedEx); (5) the ITAR reference, *i.e.*, ITAR § 125.4(b)(10), *Full-Time University Employee*.

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

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

[44] EAR § 734.11(b).

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM EXPORT CONTROL PROCEDURES

I. COMMITMENT TO EXPORT CONTROL COMPLIANCE

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

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

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

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

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

UAB is committed to export controls compliance, and the export controls compliance unit led by the Designated Official. The University Compliance staff will advise and assist faculty in conducting activities related to research and sponsored projects. More information and

resources regarding these and other regulations that impact university activities can be found at www.uab.edu/exportcontrol or by contacting the University Compliance Office, at 205-996-6540.

II. UNIVERSITY EXPORT CONTROLS ADVISORY GROUP

The University Export Controls Advisory Group is appointed by the University Empowered Official and includes liaisons to the academic units from the Provost's Office and to related business operations from the Office of Business Affairs. The University Export Controls Officer resides in the University Compliance Office, and chairs the Advisory Group.

The initial charge of the UAB Export Controls Advisory Group to address and resolve issues related to export controls that may arise from time to time, and to advise the University Empowered Official on policies, procedures and necessary institutional actions that will strengthen institutional compliance with export control regulations. In addition, the Advisory Group will develop and assist the University Export Controls Officer in the implementation of programs aimed at:

- Informing the university community on export control regulations, sanctions and embargoes;
- Implementing a university-wide export controls compliance program;
- Facilitating communication regarding export control compliance and implementation of procedures with the various constituencies on campus including, but not limited to: the deans, associate deans for research, center directors, international programs office, and administrative offices; and
- Conveying to constituencies the importance of compliance with the regulations, licenses, and agreed upon procedures, and the penalties for non-compliance.

III. KEY ACTORS RESPONSIBLE FOR EXPORT CONTROL COMPLIANCE

A. EMPOWERED OFFICIALS

The University Compliance Officer is the UAB Empowered Official for Export Control matters. In this capacity, the Empowered Official has the authority to represent the university before the export control regulators in matters related to registration, licensing, commodity jurisdiction requests, or voluntary disclosures. While certain oversight functions may be delegated, only the Empowered Official has the power to sign such paperwork and bind the university in any proceeding before DDTC, BIS, OFAC, or any other government agency with export control responsibilities.

B. UNIVERSITY DESIGNATED OFFICIAL

The University Designated Official has a dual reporting relationship with the University President and the Vice Provost for Administration and Quality Improvement. The Designated

Official has the authority and the responsibility for implementing the procedures set forth in this Export Compliance Program document. The Designated Official manages the following export control-related process:

1. Identification of areas at UAB relative to research and other activities that are impacted by export control regulations;

2. Development of control procedures to ensure the university remains in compliance;

3. Recommendation of procedures to the senior UAB administration to strengthen UAB's compliance;

4. Education of inventors, principal investigators, centers, and academic units about export control regulations and procedures followed at UAB;

5. Education of other units within UAB such as Accounting, Purchasing, Travel, International Programs, Human Resources, and Technology Transfer about export control regulations and procedures followed at UAB;

6. Monitoring and interpretation of key legislation;

7. Assisting others to facilitate understanding and compliance with export controls;

8. Conducting training and outreach on export controls;

9. Assisting investigators, researchers and offices within UAB when research or research results are export controlled;

10. Seeking legal assistance when uncertain about classification and in filing license applications; and

11. Monitoring the development of a Technology Control Plan ("TCP") for each export-controlled project consistent with these procedures to aid the principal investigator ("PI") in meeting his or her export control responsibilities.

C. OFFICE OF SPONSORED PROJECTS

The Office of Sponsored Programs (OSP) provides assistance and expertise with export controls by working closely with the UCO to identify export control issues and providing support for their solution in the following areas:

1. Provides assistance to PIs in reviewing the terms of a sponsorship agreement or grant to identify restrictions on publication and dissemination of the research results, and to help PIs negotiate out such restrictions;

2. Completes Export Control Checklists for every project and sends them to the UCO for review if export controls issues are flagged;

3. Is responsible for maintaining a centralized database of all documentation relating to a research project or education activity; and

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

The UCO will conduct training sessions for the university community and coordinate the maintenance of an export controls website.

D. KEY UNIVERSITY MANAGERS

Academic deans, directors, and department heads share the responsibility of overseeing export control compliance in their respective schools, departments, centers, or institutes and supporting the UCO in implementing procedures as deemed necessary by the UCO for export control compliance.

In addition, the directors of other offices or units on campus including, but not limited to: Accounting, Environmental Health and Safety, Human Resources, International Programs, Technology Commercialization, and Travel share the responsibility of implementing the export compliance program.

E. PRINCIPAL INVESTIGATOR ("PI")

PIs have expert knowledge of the type of information and technology involved in a research project or other university activity, such as presenting at conferences, and discussing research findings in class with fellow researchers or collaborators. PIs must ensure that they do not disclose controlled information or transfer controlled articles or services to a foreign national without prior authorization as required. To meet his or her obligations, each PI:

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

2. must assist the UCO to classify the technology involved in the research or other university activity;

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

4. must, if undertaking an export controlled project, brief the students and other researchers involved in the project of their obligations under export controls; and

5. cooperate with the UCO in developing the TCP of which the PI has the responsibility to follow and implement. The TCP template is located at Appendix C or www.uab.edu/exportcontrol.

IV. EXPORT CONTROL ANALYSIS

An export control analysis should be performed when a PI submits a proposal, receives an award, or changes the scope of an existing project.

A. INITIAL REVIEW

The OSP performs the initial review by completing the Export Control Checklists in Appendices A and B. The OSP will look for the following red flags indicating possible export control issues:

1. references to U.S. export regulations (beyond a mere statement to comply with the law);
2. restrictions on publication or dissemination of the research results;
3. pre-publication approval from sponsor;
4. proprietary or trade secret claims on project results;
5. restriction of access or participation to U.S. citizens only;
6. involvement of foreign sponsors or collaborators;
7. travel, shipping, or work performed outside the U.S.;
8. military applications of the project results; or
9. funding from the Department of Defense, the Department of Energy, the Army, the Air Force, the Naval Office, NASA, the National Reconnaissance Office, or other U.S. government agencies

B. FINAL REVIEW

If the initial review flags a possible export controls issue, the project will be referred to the UCO for final review. Upon completing the final review, the UCO will advise the PI concerning the export controls which apply to the project, the restrictions on access by foreign persons, and any other relevant requirements pursuant to ITAR and EAR.

V. TECHNOLOGY CONTROL PLAN

A. DEVELOPMENT

If the UCO determines a project is export controlled, the UCO will work with the PI to develop and implement a TCP to secure the controlled technology from access by unlicensed non-U.S. citizens. The TCP will include:

1. a commitment to export controls compliance;

2. identification of the relevant export control categories and controlled technologies;

3. identification of the project's sponsors;

4. identification and nationality of each individual participating in the project;

5. appropriate physical and informational security measures;

6. personnel screening measures; and

7. appropriate security measures for and following project termination.

B. APPROPRIATE SECURITY MEASURES

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

- Laboratory Compartmentalization**.** Project operation may be limited to secured laboratory areas physically shielded from access or observation by unauthorized individuals. These areas must remain locked at all times.

- Time Blocking. Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access.

- Marking. Export controlled information must be clearly identified and marked as export-controlled.

- Personnel Identification. Individuals participating in the project may be required to wear a badge, special card, or other similar device indicating their access to designated project areas. Physical movement into and out of a designated project area may be logged.

- Locked Storage. Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key-controlled access. Soft and hardcopy data, lab notebooks, reports, and other research materials should be stored in locked cabinets.

- Electronic Security. Project computers, networks, and electronic transmissions should be secured and monitored through User Ids, password controls, 128-bit Secure Sockets Layer encryption or other federally approved encryption technology. Database access should be managed via a Virtual Private Network.

- Confidential Communications. Discussions about the project must be limited to the identified and authorized project participants, and only in areas where unauthorized individuals are not present. Discussions with third party sub-contractors must occur only under signed agreements which fully respect the non-U.S. citizen limitations for such disclosures

C. TRAINING & CERTIFICATION

Before any individual may observe or access the controlled technology, he or she must be briefed on the procedures authorized under the TCP, certify his or her agreement to comply with all security measures outlined in the TCP, and have his or her certification authorized by the UCO or OSP. Appendix C provides UAB's template for TCP briefing and certification.

If his or her project is awarded, regardless the project's nature, each PI will receive a PI Memo describing export controls. The PI Memo is provided in Appendix D.

VI. LICENSING

If a project is export controlled and a license is needed to involve a foreign national, an Empowered Official may apply for an export license to allow the disclosure of information to foreign students and researchers. Note that each foreign student must be specifically licensed for each controlled project. Also note that a TCP, as described in Section IV above, must be implemented. The UCO, in coordination with the AVPD:OSP and outside legal counsel, will prepare and sign the necessary documentation for obtaining a license.

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

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

A *License Exception*[45] may be available for EAR controlled items, technology, or software if the individual travelling outside the U.S. can certify that he or she:

1. will ship or hand-carry the items, technology, or software for UAB business only;
2. will return or certify the destruction of the items, technology, or software within 12 months of leaving the U.S.;
3. will keep the items, technology, or software within his or her effective control;
4. will take necessary security precautions to protect against the unauthorized export of the technology; and
5. will not ship or hand-carry the items, technology, or software to a Iran, Syria, Cuba, North Korea, or Sudan[46] without first consulting with the UCO.

A *License Exemption*[47] may be available for ITAR controlled technical data transmitted outside the U.S. if the individual transmitting the technical data can certify that:

1. the technical data is to be used overseas solely by a U.S. person(s);
2. the U.S. person overseas is an employee of UAB or the U.S. Government and is not an employee of a foreign subsidiary;

[45] *See* 15 C.F.R. § 740.1.
[46] This list is subject to change. For most current list, see 15 C.F.R. § 742.1.
[47] *See* 22 C.F.R. § 125.4.

3. if the information is classified, it will be sent overseas in accordance with the requirements of the Department of Defense Industrial Security Manual; and,
4. no export will be made to countries listed by 22 C.F.R. § 126.1.[48]

Please note that other exceptions or exemptions may be available.

Any individual intending to travel or transmit controlled data outside the U.S. should first consult with the UCO. All exceptions or exemptions must be documented with the UCO and the record maintained for at least five years after the termination of the project or the travel return date.

VIII. TRAINING PROGRAMS

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

The UCO will prepare updated training materials and will ensure that employees or students engaged in an export controlled project receive the appropriate briefing. The UCO will also maintain records of training or briefings provided. A basic online export control course is available to the university community by logging onto the Collaborative Institutional Training Initiative (CITI) website at: http://www.citiprogram.org.

Academic deans, directors, or department heads will assist the UCO in implementing the export control training sessions or briefings relative to their respective schools, departments, centers, or institutes. In addition, the directors of other offices or units on campus including, but not limited to: Accounting, Environmental Health and Safety, Human Resources, International Programs, Technology Commercialization, and Travel will assist the UCO in implementing the export control training sessions or briefings.

IX. RECORDKEEPING

UAB's policy is to maintain export-related records on a project basis. Unless otherwise provided for, all records indicated herein shall be maintained consistent with the UAB record retention policy, and shall be retained no less than five years after the project's TCP termination date or license termination date, whichever is later.

If ITAR-controlled technical data is exported under an exemption, certain records of the transaction must be kept even beyond UAB's five year retention period.[49] Those records include:

1. a description of the unclassified technical data;
2. the name of the recipient /end-user;

[48] The full list of proscribed countries may be found at http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_126.pdf.
[49] *See* 22 C.F.R. §§ 122.5 and 123.26.

3. the date / time of export;
4. the method of transmission (*e.g.*, e-mail, fax, telephone, FedEx); and
5. the exemption under which the export took place.

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

BIS has specific record-keeping requirements.[50] Generally, records required to be kept by EAR must be kept for a period of five years from the project's termination date. However, if BIS or any other government agency makes a request for such records following a voluntary self-disclosure, the records must be maintained until the agency concerned provides written authorization otherwise.

X. MONITORING AND AUDITING

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

XI. DETECTING AND REPORTING VIOLATIONS

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

Any individual who suspects a violation has occurred must immediately notify an Empowered Official in the UCO, and only an Empowered Official. The UCO will then send an initial notification about the suspected violation to the appropriate government agency.[51] The UCO will conduct an internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. Once the review is complete, the UCO will provide the government agency with a supplementary letter with a thorough narrative account of:

1. the project's description and background;

2. a description of the suspected violation;

3. which items and controlled categories were involved;

4. which dates the violations occurred on;

[50] *See* 15 C.F.R. § 762.6.
[51] For EAR violations, see 15 C.F.R. § 764.5. For ITAR violations, see 22 C.F.R. § 127.12(c).

5. which countries were involved;

6. who was involved and their citizenships;

7. an explanation of why the violation occurred; and

8. any corrective actions taken; and

9. UAB's commitment to export controls compliance.

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

XII. DISCIPLINARY ACTIONS

UAB employees responsible for export controls compliance or participating in export-controlled projects must be aware of the substantial criminal and civil penalties imposed for violation of the export regulations including personal liability, monetary fines and imprisonment.

XIII. EMPLOYEE PROTECTION

No individual shall be punished solely because he or she reported what was reasonably believed to be an act of wrongdoing or export control violation. However, a UAB employee will be subject to disciplinary action if the employee knowingly fabricated, knowingly distorted, or knowingly exaggerated the report.

List of Abbreviations

OSP	Office of Sponsored Programs
BIS	Department of Commerce Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
DDTC	Department of State Directorate of Defense Trade Controls
EAR	Export Administration Regulations
ECCN	Export Control Classification Number
UCO	University Compliance Office in Office of Sponsored Projects
ITAR	International Traffic in Arms Regulations
OFAC	Department of the Treasury Office of Foreign Assets Control
OSP	Office of Sponsored Programs
PI	Principal Investigator
SDN List	Specially Designated Nationals and Blocked Persons List
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
USML	United States Munitions List
UAB	The University of Alabama at Birmingham

APPENDIX A

Specialist initials:_____ Date:_____ OSP No:_____ PI Name:_____

PROPOSAL EXPORT CONTROL REVIEW

A. Visual Compliance Check

Screen all PIs, Co-PIs, consultants and all key individuals who are at UT and are pertinent to the proposal at *Fuzzy Level 2*. (A screening of subcontractors will be done at the award stage.) Choose the appropriate category in the drop-down menu under Comments and add the OSP number in the blank box to the right of Comments. If there is a "hit," reviewer will then screen at *Exact* level. If there is a "hit" on the *Exact* level, print and take to Courtney Frazier Swaney, Assistant Director, or Export Control Officer (UCO) for further determination.

☐ **Yes** ☐ **No**

Date Completed:_____

B. Is there anything associated with this proposal that has an obviously military nature?

☐ **Yes*** ☐ **No**

C. Guidelines reference U.S. export regulations or security restrictions (beyond a mere adherence to the law)?

☐ **Yes*** ☐ **No**

D. Guidelines reference the sponsor's right to approve/disapprove publication (sponsor review only is okay; approval is not)?

☐ **Yes*** ☐ **No**

E. Foreign Persons

1. Guidelines state sponsor prohibits the involvement of non-U.S. persons or persons from certain countries. ☐ **Yes*** ☐ **No**
2. Guidelines state sponsor approval is required for foreign persons. ☐ **Yes*** ☐ **No**
3. Guidelines require additional information on foreign persons. ☐ **Yes*** ☐ **No**

* ***If* Yes *to any of above for questions C. – E., the fundamental research exclusion may be lost. Please give to UCO for export review. Please write comments below and/or attach any emails.***

F. Does the project involve a foreign sponsor, foreign collaborators, and/or travel outside of the U.S.?

☐ **Yes** ☐ **No**

1. If *Yes* is selected, is the sponsor from, collaborator(s) from, or travel to, Cuba, Iran, Syria, North Korea, or Sudan? ☐ **Yes*** ☐ **No** ☐ **Place TBD**

* ***If* Yes *is selected for F.1., UCO must review. If* No *or* TBD *is selected for F.1., the PI will receive an export control memo at award and no further review is required.***

G. Does the P.I. plan to ship or take project equipment/technology outside the U.S.? ☐ **Yes*** ☐ **No** ☐ **Unknown**

* ***If* yes*, please give to UCO for export review – a license may be required.***

Please note comments below and/or attach any email correspondence to this form:

Use this form for: **(1)** New proposals/Competitive Renewals, **(2)** Supplements with a change in SOW, & **(3)** Supplements/Non-competing Continuations *without* existing Checklist in file.

Form not needed for: **(1)** Non-competing Continuations & Supplements (with no change in SOW) *with* existing Checklists in the award file.

Please check with University Compliance Office if you have questions.

PI: _____

Sponsor: _____ **APPENDIX B**

EXPORT CONTROL REVIEW CHECKLIST FOR NEGOTIATORS

This form should be completed and kept in file even if all of the answers are "No."

B. Does the statement of work, FAR clause(s), or ANY language in the agreement:

1. Give the sponsor the right to approve/disapprove publication (excluding reasonable reviews for possible patents and/or sponsor proprietary information)? ☐ **Yes** ☐ **No**
2. Reference U.S. export regulations or security restrictions (beyond a mere statement to comply with the law)? ☐ **Yes** ☐ **No**
3. Prohibit the involvement of non-U.S. persons or persons from certain countries or requires prior approval from the sponsor? ☐ **Yes** ☐ **No**
4. Require us to identify foreign nationals including their citizenship? ☐ **Yes** ☐ **No**
5. Prohibit access to project materials/data/information by non-U.S. citizens? ☐ **Yes** ☐ **No**
6. Allow the Sponsor to claim resulting information as proprietary or trade secret? ☐ **Yes** ☐ **No**
7. Restrict the dissemination of research results? ☐ **Yes** ☐ **No**
8. Indicate the project has an obvious military nature? ☐ **Yes** ☐ **No**
   - ***If yes to any of above, the fundamental research exclusion may be lost and an export control issue may exist. Finalize export control review with Export Controls Officer (UCO). Write export control review comments in the box below and/or attach any pertinent emails to this checklist.***

C. Does the project involve travel outside the U.S.? ☐ **Yes** ☐ **No**

1. If yes, is travel to Cuba, Iran, Syria, North Korea, or Sudan? ☐ **Yes** ☐ **No**
   - ***If yes to B.1, contact UCO – a license may be required.*** ☐ **N/A**

D. Does the P.I. plan to ship or take project equipment/technology outside the U.S.? ☐ **Yes** ☐ **No**

- ***If yes, contact UCO – a license may be required.*** ☐ **Unknown**

E. If this award includes a SUBCONTRACT, please answer the following questions: ☐ **No Sub (N/A)**

1. Did you screen the subcontract PI, named participants, & entity using Visual Compliance? ☐ **Yes** ☐ **No**
   a. If yes, did you receive any negative results on the subcontract PI/entity/participants? ☐ **Yes** ☐ **No**
   - ***If yes to D.1.a, please contact UCO.*** ☐ **N/A**
2. Does the prime award have any export control and/or foreign national restrictions that must be flowed down? ☐ **Yes** ☐ **No**
3. If the project has been determined to be export controlled, will any export controlled technologies or information be given to the subcontractor? ☐ **Yes** ☐ **No**
   a. If yes, is the person receiving the technologies/info a U.S. citizen? ☐ **Yes** ☐ **No**
   - ***If no (not a U.S. Citizen), contact UCO – a license may be required.*** ☐ **N/A**
4. Will any funds be given to an entity in Cuba, Iran, North Korea, Sudan, or Syria? ☐ **Yes** ☐ **No**
   - ***If yes, contact UCO – payments to these countries may require a license or may be prohibited.***

Please note comments below and/or attach any email correspondence to this form:

Negotiator: _____ Date: _____ OSP No.: _____

Use this form for: **(1)** New awards, **(2)** Amendments with change in SOW or new task order, **(3)** Teaming agreements & MOU's with foreign entity, & (**4)** Actions on awards *without* existing Checklist.

Form not needed for: **(1)** Actions on awards *with* existing Checklist, & **(2)** VSA's / MTA's / NDA's – *however, an export control review is still required for these 3 agreements!*

APPENDIX C

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM (UAB)
OFFICE OF SPONSORED PROGRAMS (OSP)
TECHNOLOGY CONTROL PLAN (TCP) CERTIFICATION

PART I

Individual Requesting and Responsible for TCP:		
Telephone Number		
E-mail Address		
Request Date		
Description of Controls (EAR/ITAR Category)		
Location(s) Covered by TCP (add additional rows if needed)	Building	
	Room(s)	
Project Personnel	List Name(s) below:	List citizenship(s) / Permanent Res. Status:
Personnel who will have access to export controlled subject matter (add additional rows if needed)		

Is sponsored research involved?	Yes/No
If yes, identify sponsor:	
OSP Link Number and projected end date of project	

Is a non-disclosure agreement involved?	Yes/No
If yes, identify the parties:	
Contact Information:	

Attachments:	Export Briefing and Certification Form(s) for each person subject to this TCP	
Approved:	_____ UAB Authorized Official Name: _____ Title: _____	_____ Date

PART II
BRIEFING AND CERTIFICATION ON THE HANDLING OF EXPORT-CONTROLLED INFORMATION

This project involves the use of Export-Controlled Information. As a result, the project implicates either the International Traffic in Arms Regulations (ITAR) under the jurisdiction of the Department of State, or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.

It is unlawful under the ITAR to send or take Export-Controlled Information out of the U.S.; disclose, orally or visually, or transfer export-controlled information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, a license may be required for foreign nationals to access Export-Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

In general, Export-Controlled Information means activities, items, and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity for military application utility. Export-Controlled Information does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of Export-Controlled Information is military or civil in nature.

Researchers may be held personally liable for violations of the ITAR and EAR. As a result, you should exercise care in using and sharing Export-Controlled Information with others. Technical information, data, materials, software, or hardware, i.e.; technology generated from this project, must be secured from use and observation by unlicensed non-U.S. citizens. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export-Controlled Information up to and including incarceration.

Security measures will be appropriate to the classification involved. Examples of security measures are (but not limited to):

- Project Personnel – Authorized personnel must be clearly identified.
- Laboratory "work-in-progress" – Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
- Marking of Export-Controlled Information – Export-Controlled information must be clearly identified and marked as export-controlled.
- Work Products – Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; preferably located in rooms with key-controlled access.
- Equipment or internal components – Such tangible items and associated operating manuals and schematic diagrams containing identified "export-controlled" technology are to be physically secured from unauthorized access.
- Electronic communications and databases – Appropriate measures will be taken to secure controlled electronic information. Such measures may include: User ID, password control, SSL or other approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.
- Conversations – Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

Department(s):
Research Project Title:

OSP No.

Sponsor:

Certification: I hereby certify that I have read and understand this Briefing, and that I understand and agree to follow the procedures outlined in the TCP. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export-Controlled Information to unauthorized persons.

Signature: Date:

PART III

TECHNOLOGY CONTROL PLAN (TCP)

1) COMMITTMENT
The University of Alabama at Birmingham (UAB) is committed to export controls compliance. The Office of Sponsored programs is responsible for implementing technology control plans as applicable. The individual responsible for and committed to ensuring compliance with this TCP is [INSERT Name of Responsible Party].

2) BACKGROUND AND DESCRIPTION OF THE USE OF CONTROLLED ITEMS AND INFORMATION
[INSERT]

3) PHYSICAL SECURITY
[INSERT description of how equipment, technology, data and other controlled information will be shielded from unauthorized persons including descriptions of relevant security systems such as badging, escorts, visitor logs and other types of building access restrictions.]

4) INFORMATION SECURITY
Controlled data are categorized under the Data Classification Standard as Category I data. All project data and other related digital materials will be strongly password-protected and encrypted using commercially available encryption technology. Guidance on utilizing encryption as a means of protecting sensitive digital data can be accessed at http://main.uab.edu/Sites/it/policies/. The computer(s) on which this data will be stored shall not be connected to any networks. When this computer has reached its usable life, the hard drive will be forensically erased or destroyed using university hard drive destruction services.

[INSERT an outline of additional measures that will be taken to ensure information access controls that will be utilized to ensure the requirements are met including use of passwords and encryption protection. The data discard policy and relevant information technology policies and procedures should be included, as well as other plans for controlling access to controlled information. These procedures should address system backup and who will have access, transmission procedures, how computers on which sensitive digital data will be stored will be sanitized upon completion of the project, and other procedures necessary to provide the necessary security. Use of laptops for storage of this data must be justified and will only be approved with additional security procedures.]

5) PERSONNEL SCREENING
All personnel with access to the controlled technology and their nationality are listed in the TCP Certification Form. [INSERT any information on the type of background check and any additional required reviews that will be employed beyond the University's standard background check procedures for all employees.]

6) TRAINING AND AWARENESS
All personnel with access to controlled information on this project have read and understand the "Briefing and Certification on the Handling of Export-Controlled Information." Additional export control training for this project may be conducted by the UCO Export Controls Officer. The UCO also provides periodic training sessions to members of the UAB community. Additionally, all personnel with access to digital data/information stored on their university computer have read and agree to follow the UAB procedures for Protecting Sensitive Digital Research Data.

7) COMPLIANCE ASSESSMENT
As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the Designated Official at mcthomas@uab.edu (205)996-6540, to the Empowered Official for export controls at www.uab.edu/exportcontrol. The Export Controls Officer may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the Export Controls Officer or the Empowered Official for export controls.

8) PROJECT TERMINATION
Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminated when the information has been destroyed or determined to be no longer export-controlled.

APPENDIX D

Export Controls Decision Tree

The questions in this Decision Tree use terminology derived from the regulations of the US Departments of State, Commerce and Treasury. These questions ask about **sharing, shipping, transmitting or transferring** any **items, information or software**. Violations of these export control regulations can lead to significant civil and criminal penalties.

- ITEMS refers to any **tangible things, equipment or hardware**.
- INFORMATION can include **technical data** such as models, formulae, engineering designs and specifications, or **technical assistance** such as training or instruction.
- SOFTWARE refers to a collection of one or more **computer programs or micro programs** in either **source code** (programming statements) or **object code** (machine-readable instructions).

Decision Tree Question #1

Are you sharing, transmitting, or transferring UAB-developed, non-commercial encryption software (1) in source code or object code (2) (including travel outside the country with such software)?

Yes ☐ No ☐

Note (1)

The sharing, shipping, transmission or transfer of almost all encryption software in either source code or object code is subject to US export regulations. (Please contact the UCO to discuss requirements associated with transmissions or transfers of UAB-generated encryption code outside of the US).

Even most publicly available "dual-use" encryption code captured by the Export Administration Regulations (EAR) requires the availability of a License Exception. A License Exception under the EAR is an authorization based on a set of criteria, which when met, allows the exporter to circumvent export licensing requirements. The release of publicly available encryption code under the EAR is generally authorized by License Exception TSU (Technology and Software - Unrestricted) whereby the exporter provides the US Government with a "one-time" notification of the location of the publicly available encryption code prior to or at the time the code is placed in the public domain. Notification **after** transmission of the code outside the US is an export control violation.

In addition, US persons are prohibited without prior authorization from providing technical assistance (i.e., instruction, skills training, working knowledge, consulting services) to a foreign person with the intent to assist in the **overseas** development or manufacture of encryption software that is subject to US Government notification or authorization. This prohibition does **NOT** limit UAB personnel from teaching or discussing general information about cryptography or developing or sharing encryption code within the United States that arises during, or results from, fundamental research.

Two License Exceptions are available for the UAB community when the tangible export of items and software containing encryption code is necessary for travel or relocation:

- License Exception TMP (Temporary Exports) allows those departing from the US on university business to take with them as "tools of the trade" UAB-owned or controlled, retail-level encryption items such as

laptops, personal digital assistants (PDAs), and cell phones and encryption software in source or object code to all countries except Sudan and Cuba, as long as the items and software will remain under their "effective control" overseas and are returned to the US within 12 months or are consumed or destroyed abroad;

- License Exception BAG (Baggage) allows individuals departing the US either temporarily (travel) or longer-term (relocation) to take with them as personal baggage family-owned retail-level encryption items including laptops, personal digital assistants (PDAs), and cell phones and encryption software in source or object code. The encryption items and software must be for their personal use in private or professional activities. Citizens and permanent resident aliens of all countries except Cuba, Libya, Syria, Sudan, North Korea and Iran may take with them as personal baggage non-retail "strong" encryption items and software to all locations except embargoed or otherwise restricted locations.

Note (2)

Source code is generally understood to mean programming statements that are created by a programmer with a text editor or a visual programming tool and then saved in a file. Object code generally refers to the output, a compiled file, which is produced when the Source Code is compiled with a C compiler. The object code file contains a sequence of machine-readable instructions that is processed by the CPU in a computer. Operating system or application software is usually in the form of compiled object code.

Decision Tree Question #2

Do you know or have any reason to believe that the item, information or software to be shared, shipped, transmitted or transferred will support the design, development, production, stockpiling or use of nuclear explosive device, chemical or biological weapons or missiles (3)?

Yes ☐ No ☐

Note (3)

US persons are specifically prohibited from engaging in activities, either directly or indirectly, that support the proliferation of nuclear explosive devices and missiles to certain countries and their nationals without an export license. Furthermore, US persons are specifically prohibited from knowingly engaging in activities that support the proliferation of chemical or biological weapons to **any** country and its nationals without an export license. Prohibited activities include direct support (through sharing, shipping, transmission or transfer), or indirect support (through financing, contracting, servicing, transportation, support or employment) that a US person knows will facilitate the proliferation of these weapons of mass destruction (WMD) in or by those countries. In addition, an individual or organization is prohibited from proceeding with a shipment, transmission or transfer of equipment or software, or from a disclosure of information, with the knowledge that an export control violation has, or is about to, occur.

Certain chemical and biological weapons agents and precursors are listed on the US Munitions List (USML) at Category XIV and on the Commerce Control List (CCL) in Category 1 at 1C350 through 1C360.

Decision Tree Question #3

Is the item, information or software provided under a Non-Disclosure Agreement or a Confidentiality Agreement (4) central to the research program and/or do the disclosure restrictions affect the ability to publish the research results?

Yes ☐ No ☐

Note (4)

Research carrying publication and dissemination restrictions may violate principles of openness in Research practices and preclude characterization of the effort as "fundamental research." As a result, you may be facing prohibitions limiting the participation of foreign persons.

"Fundamental research" is defined as basic or applied research in science or engineering, the results of which are intended to be shared with the interested scientific community or otherwise placed in the public domain. Fundamental research, by definition, is free of access, participation, or dissemination restrictions. In accord with its openness policy, UAB will undertake ONLY fundamental research.

Fundamental research is granted special status by US export regulations, such that participation by foreign persons in such research does not require export licenses to be obtained. If the research is other than "fundamental," then the conduct and results of that research may be subject to the full array of export control restrictions.

Decision Tree Question #4

Did an external sponsor, vendor, collaborator or other third party provide, under a **Non-Disclosure Agreement or a Confidentiality Agreement**[(5)], the item, information or software to be shared, shipped, transmitted or transferred?

Yes ☐ No ☐

Note (5)

A reminder about NDAs and similar confidentiality agreements:

UAB faculty may be asked to accept confidential, proprietary, or export controlled data or material as part of a research project subject to a Non-Disclosure Agreement (NDA) signed by both the discloser and the recipient. NDAs may include **licensing agreements** which limit or prohibit the disclosure or transfer of the licensed data or materials.

In addition, if you accept confidential or proprietary information subject to a Confidentiality or Non-Disclosure Agreement, and the disclosure restrictions affect your ability to publish research results, the research itself will lose its characterization as "fundamental research" for export control purposes. Should the research entail information or software identified on US export control lists, and you wish to have foreign nationals participate in the research, you may be required to obtain an export license.

Of course, if the confidential data pertains to such information as personal health, income, or other demographic data that does not have a strategic significance (and is thus not identified on US export control lists), then export control restrictions on foreign national participation would not apply. However other restrictions may apply.

Decision Tree Question #5

Is the item being shared, shipped, transmitted , or transferred a defense article(6) other than information or software on the ITAR's US Munition Lost (USML)?

Yes ☐ No ☐

Note (6)

A defense article:

1. Is specifically designed, developed, configured, adapted, or modified for a military application, and
    1. does not have predominant civil applications, and
    2. does not have performance equivalent (defined by form, fit and function) to those of an article or service used for civil applications;
2. Is specifically designed, developed, configured, adapted, or modified for a military application, and has significant military or intelligence applicability (examples are satellites, spacecraft and their subsystems, fully field-deployable systems for military use, and space-qualified for radiation hardened microcircuits); or
3. Is on the US Munitions List (USML, the US State Department ITAR list).

Decision Tree Question #6

Is the information or software being shared, shipped, transmitted, or transferred technical data (7) on the ITAR's US Munition List (USML)?

Yes ☐ No ☐

Note (7)

Technical data means:

1. Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation.
2. Classified information relating to defense articles and defense services.
3. Information covered by an invention secrecy order.
4. Software directly related to defense articles.

"Technical data" does NOT include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities, information in the public domain, or information generated in the course of performing fundamental research.

Decision Tree Question #7

Are you shipping or transferring items (8) on the commerce Control List (CCL)(9) of the Export Administration Regulations (EAR)?

Yes ☐ No ☐

Note (8)

The Commerce Control List (CCL) is maintained by the Bureau of Industry and Security (part of the US Department of Commerce) as part of the Export Administration Regulations (EAR). This list is sometimes called the "dual use" list, as the items on it may have either a military or commercial application.

Note (9)

Items on the Commerce Control List are generally designated by categories represented by the letters "A", "B", and "C" following the initial digit in an Export Control Commodity Number (ECCN). Examples are ECCNs such as 4**A**994, 5**B**001, and 1**C**351.

- "A" category = Systems, Equipment and Components
- "B" category = Test, Inspection and Production Equipment
- "C" category = Materials

Decision Tree Question #8

Are you sharing, transmitting, or transferring technology (information)(10) or software code(11) on the Commerce Control List (CCCL)?

Yes ☐ No ☐

Note (10)

The EAR defines "technology" as:

- Specific information necessary for the "development", "production", or "use" of equipment or software. Technology includes information subject to the EAR released in the form of technical assistance or technical data.
    - Technical assistance includes instruction, skills training, working knowledge, consulting services. Technical assistance may involve transfer of export controlled information.
    - Technical data includes blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.

Information that is, or will be, placed in the public domain, such as that generated by fundamental research, is not subject to the EAR and is exempt from export control regulations.

Note (11)

The EAR defines software code as a collection of one or more programs or microprograms fixed in any tangible medium of expression. Software code is comprised of source code or object code:

Source Code: A convenient expression of one or more processes that may be turned by a programming system into equipment executable form ("object code" or object language).

Object Code: An equipment-executable form of a convenient expression of one or more processes ("source code" or source language) that has been converted by a programming system.

Note: This Decision Tree and certain technical references are based primarily on the Export Control Decision Tree developed by Stanford University.

APPENDIX E

PI MEMO (distributed at award)

The United States is committed to encourage technology exchanges that are consistent with U.S. national security and nuclear nonproliferation objectives. Although most of the research and technology development UT conducts is exempt from U.S. export control regulations, we must still comply with the regulations.

An export can occur though a variety of means, including:

- shipping,
- oral communications,
- written documentation (including e-mails), and
- visual inspections of any technology, software or technical data to any non-U.S. citizen, whether here in the U.S. or abroad.

If you are doing fundamental research and the results of the research will be in the public domain, you probably will not have any export control issues unless you have a foreign national working with **controlled** (found on the Commerce Control List or the U.S. Munitions List) proprietary technology in conjunction with your research project.

You may also be working on a project that has controlled proprietary technology or the government has placed access controls on the technology, but you do not have foreign nationals involved in your research. In this situation you must have a Technology Control Plan (TCP) in place that limits access to only U.S. citizens and foreign nationals with a green card. The template TCP can be found at the following link: (http://www.uab.edu/exportcontrol).

If you are traveling with items (including your laptop) or shipping them outside the U.S. in conjunction with your project, there are export control issues to consider **and a license could be required.** In some cases, an exception or exemption to the license requirements is available; however, **regulations require the exception/exemption to be documented, and records must be kept for five years**. A detailed explanation of the exception and exemption can be found in the UAB Export Compliance Manual.

In addition, a Material Transfer Agreement may be needed (contact Hayes Lowe in the UAB Research Foundation at 205-975-0843 or halowe@uab.edu).

More information about export controls related to research, travel, and shipping can be found at the following link http://www.uab.edu/exportcontrol. Please contact the Export Controls Officer, in the University Compliance Office, at 205-996-6540, or mcthomas@uab.edu if you have questions about export controls related to your project and/or you need to implement the required documentation.