University of Virginia

Export Compliance Management Program
Manual

Revision Date: 02/10/2016
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AECA</td>
<td>Arms Export Control Act</td>
</tr>
<tr>
<td>BIS</td>
<td>Bureau of Industry and Security</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>DDTC</td>
<td>Directorate of Defense Trade Controls</td>
</tr>
<tr>
<td>EAA</td>
<td>Export Administration Act</td>
</tr>
<tr>
<td>EAR</td>
<td>Export Administration Regulations</td>
</tr>
<tr>
<td>ITAR</td>
<td>International Traffic in Arms Regulations</td>
</tr>
<tr>
<td>OEC</td>
<td>Office of Export Controls</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>PL</td>
<td>Public Law</td>
</tr>
<tr>
<td>RPS</td>
<td>Restricted Party Screening</td>
</tr>
<tr>
<td>TCP</td>
<td>Technology Control Plan</td>
</tr>
<tr>
<td>USC</td>
<td>United States Code</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE PAGE</td>
<td>1</td>
</tr>
<tr>
<td>ACRONYMS</td>
<td>2</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td>FORWARD</td>
<td>5</td>
</tr>
</tbody>
</table>

## CHAPTER 1: OVERVIEW OF U.S. EXPORT REGULATIONS

- International Traffic in Arms Regulations (ITAR)                          | 7 |
- Items Controlled Under the ITAR                                          | 8 |
- Commodity Jurisdiction                                                    | 9 |
- Exports Under the ITAR                                                    | 9 |
- Export Authorizations                                                      | 10|
- Prohibited Destinations                                                   | 11|
- Import of Defense Articles                                                | 11|
- Export Administration Regulations (EAR)                                   | 11|
- Items Controlled Under the EAR                                            | 12|
- Exports Under the EAR                                                     | 14|
- Export Authorizations                                                      | 15|
- Treasury Sanction Programs and Barred Entities                            | 17|
- Other Export Regulations                                                  | 18|

## CHAPTER 2: OTHER RESTRICTIONS

- Anti-boycott Restrictions                                                | 19|
- Jurisdiction                                                             | 19|
- What is Prohibited?                                                      | 19|
- Exceptions                                                               | 20|
- Reporting Requirements                                                    | 20|
- Restricted Parties                                                        | 21|

## CHAPTER 3: POTENTIAL PENALTIES FOR VIOLATIONS

- Defense Articles & Technical Data                                         | 23|
- EAR Controlled Technology & Anti-boycott                                  | 24|
- OFAC Sanctions                                                           | 24|
- Penalty Assessment                                                        | 25|

## CHAPTER 4: INTERSECTION OF EXPORT CONTROLS AND UNIVERSITY ACTIVITIES

- University Activities Excluded from or Not Subject to Export Control     | 26|
- Publicly Available (EAR); Public Domain (ITAR); or Information and Information Materials | 26|
- Fundamental Research (EAR & ITAR)                                        | 27|
- Educational Information (EAR) and General Principles in Science and Engineering (ITAR) | 28|
- Areas of Continuing Impact on Academic Pursuits and Activities           | 29|
- Physical Exports of Items, Including Technical Data, or Technology       | 30|
- “Deemed” Exports and Technical Data Exports in the U.S.                   | 30|
- “Defense Services” in Educational/Training Situations                    | 31|

## CHAPTER 5: UNIVERSITY OF VIRGINIA EXPORT CONTROL POLICY & RESPONSIBLE PARTIES

- Institutional Commitment                                                 | 33|
The University of Virginia’s principal and best tools for ensuring compliance with export controls are to 1) keep listed materials off Grounds if it would require a license for use by foreign national students and employees; and 2) ensure that all physical exports from the U.S. are appropriately screened, and when necessary licensed. However, the University has determined that it can and will accept export control-listed materials as well as export controlled or publication restricted projects on a case-by-case basis. When the University decides to allow listed materials on Grounds a strong control program is essential to assure continuing compliance with regulatory requirements.

It is the Office of Export Controls’ responsibility to assist university personnel with export control and licensing in support of authorized university activities to the extent permitted and allowed by the applicable laws and regulations. It is not the role of the Office of Export Controls to determine what research or other activities university research and academic personnel may or may not engage in; that determination shall fall to the individual’s department, school, and the Office of the Vice Provost for Research (research activities including graduate studies) or Provost (academic activities).

This Manual has been developed by the Office of Export Controls to describe and formalize the internal policies and procedures that comprise the University of Virginia’s Export Compliance Management Program and is intended for internal use and distribution only. Any inconsistency between the content of this manual and U.S. export control laws and regulations is unintentional; in all cases the requirements of the applicable law or regulation shall take precedence.

It is important to note that any export from the U.S. is an import to another country. It is the responsibility of the individual exporter to identify and comply with the applicable import laws and regulations of other countries when exporting on behalf of the University.

**General Notes**

The University Export Control Management Program and this Manual are designed for compliance with multiple regulatory schemes; therefore, general terms are sometimes used in place of regulation specific terms. For example, the terms “export control-listed materials” and “listed materials” are used to refer to any information/data, commodity, material, technology, software, etc., subject to export control, other than those designated as EAR99, although EAR99 materials, information, software or technology are also subject to a minimal level of export controls in certain instances. When regulation specific terms are used in this Manual the applicable citation is provided as a parenthetical reference.

A list of common acronyms used in the manual are provided on page 2.
Introduction

The United States (U.S.) has numerous laws and regulations governing the export of a wide variety of materials, goods and services; often referred to collectively as (U.S.) export controls. The responsibility to regulate and enforce export controls is a distributed function within the U.S. government involving multiple departments and agencies. Export controls apply equally to all types of institutions, organizations and individuals in the U.S. and in some instances U.S. jurisdiction extends to U.S. origin items and U.S. persons physically located outside the U.S. Foreign items may also become subject to U.S. jurisdiction once they enter U.S. commerce.

Before discussing individual export control regulations it is critical to have an understanding of what constitutes an “export”. In general terms, an export occurs whenever something leaves the boundaries of the U.S.; this obviously includes physical shipments of items and materials, but it also includes the transfer, regardless of means or method, of information. The export of information may occur during conversations (in-person, telephonic or electronic) or by e-mail, standard mail, fax, web postings, or deposit in shared servers (cloud computing) to name a few examples. When information is provided to a foreign national in the U.S. it is deemed to be an export to the individual’s country of citizenship and/or residency; such transfers are often referred to as “deemed exports”. The term “deemed export” is not universally used in the regulations, but the concept is consistent.

Understanding who constitutes a U.S. versus a foreign person is also critical to determining export control and licensing requirements. Generally speaking, the export regulations define a “person” to include both natural persons and companies, government agencies, and other organizations. A natural person is a “U.S. person” if they are a U.S. citizen, a person lawfully admitted for permanent residence in the U.S. (i.e., green card holder), or a person who is a protected individual under the Immigration and Naturalization Act1 (i.e., certain classes of asylees); the term “U.S. person” also means any entity, organization or group that is incorporated to do business in the United States, including governmental entities (federal, state or local). Although the terms are similar among the export regulations it is important to always use the specific definition provided in a given regulation when making an assessment.

The most extensive export control regulations are those associated with technology and certain types of associated technical data. U.S. law and presidential delegation of authority have assigned the control of technology exports to three principal agencies: the Directorate of Defense Trade Controls, Department of State; Bureau of Industry and Security, Department of Commerce; and the Office of Foreign Assets Control, Department of the Treasury. Each agency has its own scope of authority and implementing regulations which are briefly discussed below.

---

1 8 USC § 1324b(a)(3)
The ITAR implement authority granted to the President by §38 of the Arms Export Control Act (AECA), subsequently delegated to the Secretary of State, to regulate international trade involving military technology. Items are subject to the ITAR when they meet the policy criteria identified in ITAR §120.3 and are specifically designated by the Department of State with the concurrence of the Department of Defense. The list of designated defense articles constitutes the U.S. Munitions List (USML).

The ITAR are issued and administered by the Directorate of Defense Trade Controls (DDTC) and regulate the export of the following: [PLEASE NOTE THAT AS OF FEBRUARY 10, 2016, THE FOLLOWING DEFINITIONS ARE CURRENTLY BEING REVISED AND WILL BE PUBLISHED FOR PUBLIC COMMENT IN THE NEAR FUTURE AS PART OF EXPORT CONTROL REFORM. Please check the regulatory citation for the most recent definition.]

- **Defense Articles** - means any item or technical data that is specifically listed on the USML as well as including any forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles. Technical data may be data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items on the USML. It does not include basic marketing information on function or purpose or general system descriptions.

- **Technical Data** - means any information, other than software, which is required for the design, development, assembly, production, manufacture, operation, repair, testing, maintenance, or modification of a defense article. Technical data may include drawings, blueprints, photographs, plans, 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. It should be noted that if a U.S. government contractor makes the determination that an effort is controlled under the ITAR, all work and technical data generated for that project is subject to the ITAR, regardless of whether it may have previously existed in the public domain. Technical data also includes classified information relating to defense articles and defense services on the USML and “600-series” items controlled by the Commerce Control List of the Export Administration Regulations (EAR). Information covered by

---

2 22 CFR Parts 120 – 130.
3 22 USC 2778, Chapter 39
4 Executive Order 11958
5 ITAR § 121
6 ITAR § 120.6
7 ITAR § 120.10
an invention secrecy order and software directly related to defense articles are also considered technical data controlled under the ITAR.

- **Defense Services**\(^8\) - means providing assistance, including training, to a foreign person in the United States or abroad in the design, development, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of a defense article, as well as providing technical data to foreign persons wherever located. Defense services also include informal collaboration, conversations, or interchanges concerning technical data. Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

**Items Controlled Under the ITAR**

The USML designates particular categories and types of equipment as defense articles and associated technical data and defense services\(^9\). The USML divides defense items into 21 categories, listed below.

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

\(^8\) ITAR § 120.9
\(^9\) See ITAR § 121.1
• Category XVII: Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
• Category XVIII: Directed Energy Weapons
• Category XIX: Gas Turbine Engines and Associated Equipment
• Category XX: Submersible Vessels and Related Articles
• Category XXI: Articles, Technical Data, and Defense Services Not Otherwise Enumerated

An electronic version of the USML is available on the Department of State website under ITAR 22 CFR Part 121 at: http://www.pmddtc.state.gov/regulations_laws/itar.html.

Commodity Jurisdiction

Although DDTC has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify items. If any doubt exists as to whether an article is covered by the USML or an activity constitutes a defense service, upon written request in the form of a Commodity Jurisdiction (CJ) request, DDTC will render a decision as to the appropriate regulatory jurisdiction (EAR or ITAR)\(^\text{10}\). 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 and students should contact the Office of Export Controls for assistance when classifying an item or preparing a CJ request.

Getting the jurisdiction correct is essential to continuing compliance with the export regulations. When BIS recognizes that a Commodity Classification request involves potentially ITAR-controlled technology it will suspend the Commodity Classification review and forward the information to DDTC for a jurisdiction determination.

Exports Under the ITAR

The ITAR defines the term “export” broadly, applying it not only to exports of tangible items from the U.S., but also to transfers of intangibles, such as technology or information\(^\text{11}\). The following are examples of exports:

• Tangible Exports and Transfers
  o Shipping or taking a defense article or technical data out of the United States (this includes the electronic download of technical data from a server in the U.S. to a laptop located outside of the United States).
  o Transferring title or ownership of a defense article to a foreign person, in or outside the United States.

\(^\text{10}\) ITAR § 120.4. Instructions and required information for filing a CJ request (Form DS-4076) are available at http://www.pmddtc.state.gov/commodity_jurisdiction/index.html. You can check the status of pending CJ requests at https://dtas-online.pmddtc.state.gov/MARY/index.cfm.
\(^\text{11}\) ITAR § 120.17
- 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.

- **Intangible Exports**
  - 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.

**Export Authorization**

Registration\(^{12}\) with DDTC is required for any U.S. person or entity that manufactures, brokers, or exports defense articles or services. Only registered persons or entities may applying for a license or take advantage of certain license exemptions. Once registered, an exporter may apply for an export authorization by submitting a license application for the export of defense articles, technical data; or defense services. Most types of applications require the inclusion of various certifications and other supporting documentation depending on the specific defense article(s) to be exported, defense services to be provided, and other facts of the export.

University researchers typically become subject to the ITAR when a defense article or technical data is necessary for the conduct of research. If the university intends to involve foreign nationals in ITAR-controlled research, it must apply for a license or take advantage of certain license exemptions. Results generated using a defense article or technical data (as background or supporting information) that are not related to the further design, development, modification or use of the defense article will not themselves be subject to the ITAR if the university does not accept restrictions on dissemination of the results or the involvement of foreign nationals. In such cases the research results may be considered to be fundamental and may be accessed and used by foreign nationals. Should the university accept dissemination or foreign national restrictions on the research then the resulting data or product may also be subject to the ITAR.

The ITAR (§125.4) contain some exemptions from the general applicability of license requirements, but their applicability and usefulness for university purposes is relatively limited. University researchers wishing to use an ITAR exemption should consult with the OEC and receive a written determination of the exception prior to the export.

\(^{12}\) ITAR § 122.1
**Prohibited Destinations**

The ITAR specifically prohibits issuance of a license or use of a license exception for the export of defense articles or services to certain proscribed countries (§126.1); this prohibition includes transfers to nationals of prohibited countries. Proscribed countries, as of the date of this revision, include Belarus, Cuba, Eritrea, Iran, North Korea, Syria and Venezuela. Additionally §126.1 prohibits exports of defense articles and services to countries subject to a U.S. arms embargo, which, as of the date of this revision, includes Burma, China and the Republic of Sudan. Exports of items or technical data controlled under the ITAR are also prohibited to nationals of countries subject to United Nations Security Council embargoes. The countries currently listed under those embargoes include Cote d’Ivoire, Democratic Republic of Congo, Eritrea, Iraq, Iran, Lebanon, Liberia, Libya, North Korea, Somalia, and The Republic of Sudan. Exports to nationals of countries which the Secretary of State has determined repeatedly provide support for acts of international terrorism are also prohibited and currently, Cuba, Iran, the Republic of Sudan and Syria are currently included in that list. The list of proscribed countries changes from time to time, so the current DDTC list should be checked prior to initiating any export transaction; the list may be accessed online at: [http://www.pmddtc.state.gov/embargoed_countries/](http://www.pmddtc.state.gov/embargoed_countries/)

**Import of Defense Articles**

It is important to note that the ITAR also regulate the temporary import of defense articles. However, authority to regulate the permanent import of arms, ammunition and implements of war falls under the jurisdiction of the Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives. The list of items subject to import regulation is called the U.S. Munitions Import List (USMIL)\(^\text{13}\) which differs from the USML. All designations of articles subject to import control under §414 of the Mutual Security Act of 1954, as amended, have the concurrence of the Secretary of State and the Secretary of Defense.

**Export Administration Regulations (EAR)\(^\text{14}\)**

The EAR are issued by the U.S. Department of Commerce, Bureau of Industry and Security (BIS) under the Export Administration Act (EAA) of 1979, as amended\(^\text{15}\). The EAA is not permanent legislation and has been in lapse since August 21, 2001; since that time the authority of the EAR has been extended by Presidential Executive Orders issued under authority granted by the International Emergency Economic Powers Act (IEEPA)\(^\text{16}\).

---

\(^{13}\) 27 CFR, Part 447, Subpart C.


\(^{15}\) Public Law (PL) 96-72.

\(^{16}\) PL 95-223; 50 USC 1701 et seq.
The EAR control the export of both items and “technology”. Under the EAR, “technology” is defined as the “specific information necessary for the ‘development’, ‘production’, or ‘use’ of a product. The information takes the form of ‘technical data’ or ‘technical assistance’. Controlled ‘technology’ is defined in the General Technology Note and in the Commerce Control List.” The General Technology Note (GTN)\(^\text{17}\) states “(t)he export of ‘technology’ that is ‘required’ for the ‘development’, ‘production’, or ‘use’ of items on the Commerce Control List is controlled according to the provisions in each Category.”

“Required”, “Development”, “Production”, “Use”, “Technical data”, and “Technical assistance” are all defined terms under the EAR\(^\text{18}\) and may not have the same meaning as they do in common usage or as used in export control regulations promulgated by other federal agencies.

- **Required** (as used in the GTN and CCL Categories 4, 5, 6, and 9) – that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.
- **Development** – all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.
- **Production** – means all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance.
- **Use** (as used in all CCL categories (except for 600 series items which are most rigorously controlled and for which only one of the types of “use” will be necessary to constitute “technology”) and the GTN) – information required for the development, production, operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.
- **Technical data** – may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories.
- **Technical assistance** – May take forms such as instruction, skills training, working knowledge, consulting services. May involve the transfer of “technical data”.

**Items Controlled Under the EAR**

The term “dual-use”, which refers to items that have both military and civilian applications, has often been used to describe the scope of technologies that are subject to the EAR but that term is not entirely accurate as the EAR also control items with purely civilian applicability and military items that have been formally transferred from the ITAR. Items or technologies are subject to the regulatory authority of the EAR if described in §§734.2 through 734.5.

\(^{17}\) EAR § 774, Supplement No. 2  
\(^{18}\) EAR § 772
Generally, all items of U.S.-origin, or physically located in the United States, are subject to control under the EAR unless subject to the jurisdiction of another agency. Foreign manufactured goods are generally exempt from the EAR re-export requirements provided they contain less than a de minimis level of U.S. content by value (10% to embargoed countries; 25% to all other destinations).

Items subject to specific control and licensing policies are identified in an Export Control Classification Number (ECCN) on the Commerce Control List (CCL). Each ECCN is composed of five alpha-numeric characters; a number, followed by a letter, followed by three additional numbers. The first number designates which one of the ten CCL categories of technology captures the item:

- Category 0 - Nuclear Materials, Facilities, and Equipment [and Miscellaneous Items]
- Category 1 - Special Materials and Related Equipment, Chemicals, “Microorganisms,” and “Toxins”
- Category 2 - Materials Processing
- Category 3 - Electronics
- Category 4 - Computers
- Category 5 (Part 1) - Telecommunications
- Category 5 (Part 2) – Information Security
- Category 6 - Sensors and Lasers
- Category 7 - Navigation and Avionics
- Category 8 - Marine
- Category 9 - Aerospace and Propulsion

The first letter in the ECCN (second alpha-numeric character) indicates the type of item controlled. Within each of the nine ECCN categories listed above the controlled items are divided into the following five (A through E) groups:

- Group A - Equipment, Assemblies and Components. These are essentially saleable commodities; finished or unfinished goods ranging from high-end microprocessors to airplanes, to ball bearings.

- Group B - Test, Inspection and Production Equipment. These items are generally referred to as 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.

- Group C - Materials. This includes certain alloys and chemical compounds. It also includes controlled biologics and toxins.

- Group D - Software. This includes software specifically associated with particular controlled commodities or manufacturing equipment, as well as any software containing encryption and the applicable source code.
Group E - Technology. As defined in the EAR, “technology” includes both technical data, and services. Unlike the International Traffic in Arms Regulations, no distinction is made between technical data and “know how” or assistance. However, the EAR may apply different standards to technology for “use” of a product than for the technology for the “development” or “manufacture” of the product.

The third character or second digit listed in the ECCN is a number from the following categories of “Reasons for Control”, listed below, which designate the type of controls associated with the items contained in the particular entry.

- 0: National Security reasons (including Dual Use and Wassenaar Arrangement Munitions List) and Items on the NSG Dual Use Annex and Trigger List.
- 1: Missile Technology reasons
- 2: Nuclear Nonproliferation reasons
- 3: Chemical & Biological Weapons reasons
- 5: Items warranting national security or foreign policy controls at the determination of the Department of Commerce.
- 6: “600 series” controls items because they are on the Wassenaar Arrangement Munitions List (WAML) or formerly on the U.S. Munitions List (USML).
- 9: Anti-terrorism, Crime Control, Regional Stability, Short Supply, UN Sanctions, etc.

Reasons for Control are not mutually exclusive so numbers are assigned in order of precedence. So, if an item is controlled for both National Security and Missile Technology reasons, the entry’s third digit will be a “0”. If the item is controlled only for Missile Technology the third digit will be a “1”.

Items that are subject to the EAR but not to any specific control or licensing policies are not described by a specific ECCN on the CCL; such items are designated EAR99. Items or technologies identified as EAR99 are subject to the lowest level of control, meaning they can be exported to most countries (i.e. those not subject to an embargo) without a license provided they are not going to a prohibited or restricted end-user or being used for a prohibited end-use.

When licensing requirements exist for items listed on the CCL, they may often be overcome by one or more of the license exceptions (essentially pre-authorization to export) carved out in the EAR (Section 740). However, significant due diligence and recordkeeping is require to insure compliance with applicable requirements.

Licensing and license exceptions are discussed in more detail in later sections.

Exports Under the EAR

The EAR control both the actual shipment or transmission of controlled items out of the U.S. (export) and any subsequent transfer of controlled items originally exported from the U.S. to a third country (re-
The terms “deemed export” and “deemed re-export” are used respectively to refer to the release of “technology” to a foreign national in the U.S. and the release of technology by a foreign national who has been licensed to receive it to the national of another foreign country. Such transfers are “deemed” to be exports to the foreign national’s home country regardless of the fact that they occur in the U.S. or abroad, in the case of deemed re-exports.

Export Authorizations

Once it has been determined that a license is required, an exporter can apply for export authorization from BIS through their online licensing system SNAP-R or take advantage of an available license exception. The University has an institutional registration for SNAP-R that is managed by the Office of Export Controls which submits license applications in support of University activities.

The EAR contain 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.

Once an item has been classified under a particular ECCN heading, the next step is to determine whether a license is required to export the specific item to the destination country. The following three steps describe the process by which a user can first determine licensing requirements and then whether or not an exception is available.

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

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

---

19 EAR § 772
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” and indicates that the control applies to the entire entry “AT Column 1” which refers to the Country Chart. Items may be controlled for more than one reason so it is important to identify all applicable reasons for control.

(2) Apply Country Chart. Once an item is identified as having specific control 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 applies.

(3) Assess License Exceptions. The EAR contains a number of exceptions. Determining whether a particular exception applies requires review of the specific application details, as well as the notes on applicable license exceptions following the ECCN entry. Possible license 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.
- TMP - Certain temporary exports, re-exports, or imports, including items moving through the U.S. in transit.
- RPL - Certain repair and replacement of 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.
- STA - Strategic Trade Authorization which allows for exports to or for ultimate end use by the governments of close allies.
- SCP – Support for the Cuban People

---

20 Supplement No. 1 to EAR § 738
21 EAR § 740
22 Supplement No. 1 to EAR 740 contains the Country Group Listings (A:1-6; B; C (reserved); D:1-5; and E:1-2)
Each license exception is unique, so it is imperative to examine each closely to determine whether or not it fits the circumstances of the proposed export. Exceptions particularly useful to universities, as well as licensing procedures, are described in detail in “Areas of Continuing Impact on Academic Pursuits and Activities” below. University researchers wishing to use a license exception should consult with the OEC and receive a written determination of the exception prior to the export.

**Treasury Sanction Programs and Barred Entities**

The U.S. is a party to a wide range of embargoes and trade sanctions. In some cases the U.S. may issue an embargo or sanctions regulations solely in support of U.S. foreign policy (e.g. Cuban Assets Control Regulations), while in other cases they implement of U.S. responsibilities under a multilateral agreement (e.g. United Nations and North Atlantic Treaty Organization sanctions or initiatives). Treasury sanction programs may be list-based (e.g. narcotics trafficking, weapons of mass destruction proliferation, and global terrorism) or country-based (e.g. Iran, Cuba, and North Korea). U.S. embargoes and trade sanctions are administered and enforced primarily by the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC).

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.

OFAC sanctions are issued under the authority of the International Emergency Economic Powers Act of 1977 (IEEPA), with the exception of the embargoes on Cuba and North Korea which are issued under the authority of the Trading with the Enemy Act of 1917 (TWEA). The 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, including but not limited to Burma, Liberia, and Zimbabwe; this list is not complete and is subject to change in response to new foreign policy decisions or directives, please visit [http://www.treas.gov/offices/enforcement/ofac/](http://www.treas.gov/offices/enforcement/ofac/) and click the “Resources” tab for a full list of U.S. sanction programs.

While most sanctions are administered by OFAC, BIS has jurisdiction over certain export prohibitions (via “embargo” regulations), such exports to Syria. 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. Each sanction or embargo program in the FACR is independent and unique. You cannot expect that sanctioned activities identified in the Iranian Assets Control Regulations will be the same as those identified in the Sudanese

---

23 31 CFR Subtitle B, Chapter V  
24 50 USC §§ 1701-1706  
25 12 USC § 95a  
26 15 CFR § 746
Sanction Regulations. Similarly, an activity that may be eligible for a general license under one sanction regulation may not be licensable or may require a specific license in another.

**Other Export Regulations**

Other agencies with regulatory authority over exports include, but are not limited to, the following:

- **Department of Justice, Drug Enforcement Administration, Office of Diversion Control**
  - Scope: drugs (of abuse), chemicals and precursors
  - Regulations: 21 CFR Parts 1311-1313

- **Food and Drug Administration**
  - Scope: drugs, biologics, medical devices and investigational drugs
  - Regulations: 21 U.S.C. 301 et seq. and 21 CFR 312.1106
  - Agency Website: [http://www.fda.gov/](http://www.fda.gov/)

- **Department of the Interior, Chief Office of Management Authority, Fish and Wildlife Service**
  - Scope: endangered species
  - Regulations: 50 CFR 17.21, 17.22, 17.31, 17.32.
  - Agency Website: [http://www.fws.gov/](http://www.fws.gov/)

- **Nuclear Regulatory Commission, Office of International Programs**
  - Scope: nuclear materials and equipment
  - Regulations: 10 CFR part 110

- **Department of Energy, Office of Export Control Policy & Cooperation**
  - Scope: Nuclear Technologies and Services Which Contribute to the Production of Special Nuclear Material
  - Regulations: 10 CFR part 810
  - Agency Website: not available

Items exclusively controlled for export or re-export by the Departments of State, Treasury, and Energy as well as those controlled by the Nuclear Regulatory Commission and the Patent and Trademark Office are excluded from the scope of the EAR\(^27\). Control by a single federal agency is typical; however, situations may arise where licenses from two or more agencies may be required to support for the same University activity.

---

\(^27\) EAR § 734.3(b)(1)
Anti-boycott Restrictions

The anti-boycott rules are found in the 1977 amendments to the Export Administration Act (EAA) and the Ribicoff Amendment to the 1976 Tax Reform Act (TRA) and 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 and the applicable regulations are at 15 C.F.R. § 760. The TRA does not prohibit specific conduct; rather, it denies tax benefits for certain types of boycott related activities.

Anti-boycott restrictions are most likely to arise in dealings with entities in Arab League countries. As of this writing, Iraq, 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 currently listed, but its status with respect to the future lists remains under review by the Department of Treasury. Egypt and Jordan have ceased participating in the boycott. There are strict reporting requirements even where the U.S. person refuses to participate in a requested boycott action; forms for reporting requests for restrictive trade practices are available on BIS's Anti-boycott webpage.

Jurisdiction

The anti-boycott 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 the affiliate is controlled by the U.S. company and the transaction involves shipment of goods to or from the U.S.

What is Prohibited?

The U.S. 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.

---

28 PL 95-52 § 201(a)
29 The Ribicoff Amendment to the Tax Reform Act (PL 94-455) added Section 999 to the Internal Revenue Code (26 USC § 1 et seq.).
30 See 26 CFR § 7.999-1 for the Implementing tax regulations.
• Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin, or nationality.

• Agreements to furnish or actual furnishing of information about business relationships with Israel or with blacklisted companies.

• Agreements to furnish or actual furnishing of 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.

Exceptions

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.

Reporting Requirements

The EAR requires U.S. persons to report requests they have received to comply with, further, or support an unsanctioned foreign boycott on a quarterly basis. Links to the required report forms as well as the regulations and examples of boycott requests are available on BIS’s Anti-boycott Compliance webpage (http://www.bis.doc.gov/index.php/enforcement/oac). The Office of Antiboycott Compliance has also set up an advice line for questions about the anti-boycott rules, which can be reached at (202) 482-2381. The U.S. Internal Revenue Service (IRS) also requires U.S. taxpayers to report operations in or relating to boycotting countries and nationals and requests to cooperate with boycott activities.

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.

---

33 EAR § 760.5
Restricted Parties

Several U.S. Government agencies maintain one or more lists of individuals or entities that are barred or otherwise restricted from entering into certain types of transactions with U.S. persons. The following lists are specifically applicable to export controls and must be screened to ensure that the university does not engage in a transaction with a barred entity.

- **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](http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml).

- **Persons Named in General Orders**\(^{35}\). As of this writing, General Order No. 1 establishes a 24-month validity period for all reexport authorizations; General Order No. 2 contains the provisions of the U.S. embargo on Syria. The controls for exports and reexports to Syria are set forth in §746.9 of the EAR; General Order No. 3, dated July 22, 2015, provides that all conditions that apply to Country Group E:1, as specified in Supplement N. 1 to part 740 of the EAR, on licenses issued prior to July 22, 2015 and that are in effect on that date, are revised to apply to Country Groups E:1 and E:2 as specified in Suppl. No 1 to part 740 of the EAR; General Order No. 4 is “reserved”; and General Order No. 5, dated April 16, 2013, provided authorization for items the President Determines No Longer Warrant Control under the USML which will be transferred to the Commerce Control List (CCL) as final rules become published. A link to the General Orders is available at: [http://www.bis.doc.gov/index.php/forms-documents/doc_view/413-part-736-general-prohibitions](http://www.bis.doc.gov/index.php/forms-documents/doc_view/413-part-736-general-prohibitions).

- **AECA Debarred List.** Issued by the Department of State, this list identifies entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services. The list is available at: [http://www.pmddtc.state.gov/compliance/debar.html](http://www.pmddtc.state.gov/compliance/debar.html). Note that the number of countries subject to a U.S. arms embargo is not the same as those subject to OFAC embargoes. See for a list of embargoes [http://www.pmddtc.state.gov/embargoed_countries/index.html](http://www.pmddtc.state.gov/embargoed_countries/index.html).

- **Denied Persons List.** Identifies those individuals and entities that have had their export privileges revoked or suspended by BIS. Dealing with a party on this list is prohibited only if it would violate the terms of the denial order. The list includes a reference to the Federal Register notice publishing the denial order and is available at: [http://www.bis.doc.gov/dpl/default.shtm](http://www.bis.doc.gov/dpl/default.shtm). It is important to note that denial orders may be either “standard” or “non-standard” with “standard” orders issued after 27 August 2002 conforming to the language posted at [http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list/12-policy-guidance/list-parties-of-concern/321-the-denied-persons-list-standard-order](http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list/12-policy-guidance/list-parties-of-concern/321-the-denied-persons-list-standard-order). As

---

\(^{35}\) EAR § 736, Supplement No. 1
the name implies, “non-standard” denial orders contain different terms so reviewing the full denial order is critical when evaluating a proposed transaction involving a party subject to a “non-standard” order. All denial orders are published in the Federal Register, which is accessible at [http://www.gpo.gov/fdsys/](http://www.gpo.gov/fdsys/).

- **Entity List.** Parties whose presence in a transaction can trigger a license requirement beyond those identified elsewhere in the Export Administration Regulations (EAR). The list provides the specific license requirements and policy that apply to each listed party. The list is available at: [http://www.bis.doc.gov/entities/default.htm](http://www.bis.doc.gov/entities/default.htm).

- **Unverified List.** These are foreign “persons” for which BIS has been unable to verify the nature of their operations. Dealings with these entities are not prohibited; however, their presence in a transaction is a “red flag” and should be resolved before proceeding with the transaction. The list is available at: [http://www.bis.doc.gov/enforcement/unverifiedlist/unverified_parties.html](http://www.bis.doc.gov/enforcement/unverifiedlist/unverified_parties.html).

- **Nonproliferation Sanctions.** These are sanctions against foreign individuals, private entities, and governments that engage in proliferation activities. The Department of State maintains a list of current sanctions at: [http://www.state.gov/t/isn/c15231.htm](http://www.state.gov/t/isn/c15231.htm).

To facilitate the restricted party screening process the U.S. Government has created a Consolidated Screening List that incorporates the entries on all of the lists identified above. The Consolidated Screening List is available for download at [http://export.gov/ecr/eg_main_023148.asp](http://export.gov/ecr/eg_main_023148.asp).

In addition to screening against export-related restriction lists, the University must also screen parties against the **Excluded Parties List System** when the activity or transaction involves Federal funds. The parties on the EPLS are entities that have been barred from contracting (procurement, non-procurement, and reciprocal programs) with U.S. Government agencies. All companies and universities contracting with the U.S. Government, either as prime or subcontractors, must comply with these prohibitions. The EPLS was available up until 2012 at: [http://www.epsl.gov/](http://www.epsl.gov/) but then moved to the System for Award Management (SAM).36

The University of Virginia uses Visual Compliance™, a product of eCustoms Inc., to expedite screening of these and other lists. Visual Compliance maintains an audit trail of all restricted party screenings and has a dynamic screening function that rescreens all entries daily and provides a notification if there is ever a change in the status of a previously screened party. The Director, Office of Export Controls, is the Visual Compliance Account Manager for UVA and receives all change of status notifications and has access to all prior screening transactions for audit purposes.

---

CHAPTER 3: POTENTIAL PENALTIES FOR VIOLATIONS

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 criminal penalties, civil penalties, or both. Although maximum penalties are identified in the regulations, the listed figures are per violation providing the opportunity for the actual penalty imposed to be 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.

Defense Articles & Technical Data

The Arms Export Controls Act (AECA) and the ITAR provide that willful (i.e. criminal) violations of the defense controls can be fined up to $1,000,000 per violation, or twenty years of imprisonment, or both. The Secretary of State may also assess civil penalties, which may not exceed $500,000 per violation. 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 are subject to seizure, forfeiture and disposition. Additionally, 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.

While criminal prosecution is relatively rare, many major U.S. companies have been assessed significant civil penalties. For example, following an extensive export investigation ITT Corporation, a leading manufacturer of night vision equipment for the U.S. military, received a three-year debarment of the company's Night Vision Division. As part of their consent agreement ITT also agreed to pay a total of $100 million for violations of defense export laws. To date, this is one of the largest penalties ever paid in a criminal or civil case.

The Department of State encourages persons that believe they may have violated any export control provision of the AECA or any regulation, order, license, or other authorization issued under its authority

37 22 USC § 2778(c)
38 22 CFR § 127.3
39 22 USC § 2778(e) and 22 CFR § 127.10
40 22 CFR § 127.6
41 22 USC § 2778(g) and 22 CFR § 127.7
42 A thorough discussion of penalties imposed under the ITAR is available in “Monograph on U.S. Defense Trade Enforcement” by John C. Pisa-Relli (Feb 2007).
to voluntarily disclose the information to DDTC. Voluntary disclosure may serve as a mitigating factor in the determination of administrative penalties.

**EAR Controlled Technology & Anti-boycott**

Violations of the EAR are subject to both criminal and administrative penalties. Fines for export violations, including anti-boycott violations, can be as high as $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 up to 20 years in prison, and administrative penalties may include the denial of export privileges. For many violators a denial order is probably the most serious sanction as it would bar a U.S. company from exporting or bar a foreign entity from buying U.S. origin products for a specific period of time, typically several years.

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.

**OFAC Sanctions**

Exporter may be subject to a maximum civil penalty of $250,000 per violation under OFAC regulations, with the exception of exports to Cuba. Violations of the Cuban sanctions are subject to a maximum penalty of $65,000 per violation. The U.S. Government may also pursue criminal prosecution if violations are willful and knowing. Penalties for criminal violations may reach $1,000,000 per violation and imprisonment of up to 20 years. In addition to OFAC penalties, egregious conduct by the violator may result in BIS suspending export privileges.

---

44 22 CFR § 124.12
45 These violations are based on the Export Administration Act of 1979, as amended (50 USC app. §§ 2401-2420), and inflation adjustments made in 15 CFR § 6.4. From 21 August 1994 through 12 November 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 USC §§ 1701-1706 (IEEPA). On November 13, 2000, the Act was reauthorized by P.L. 106-508 (114 Stat. 2360 (2000)) and it remained in effect through 20 August 2001. Since 21 August 2001 the Act has been in lapse and the President, through Executive Order 13222 of 17 August 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 9 March 2006 (P.L. 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, P.L. 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.
46 The Bureau of Industry and Security issues an annual publication entitled “Don’t Let This Happen to You! Actual Investigations of Export Control and Antiboycott Violations” on its website (http://www.bis.doc.gov/index.htm); the July 2015 edition is the most recent and is available at http://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance, click on the title “Don’t Let This Happen to You” under the Recommended Links on the left side of the web page.
47 Most economic sanction regulations penalties are set under IEEPA. See supra note 22.
48 The embargo of Cuba was promulgated under the authority of the Trading with the Enemy Act (TWEA).
Penalty Assessment

DDTC\textsuperscript{49}, BIS\textsuperscript{50}, and OFAC consider a number of factors, both aggravating and mitigating, when assessing penalties. 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.

The weight given to any given factor is left to the discretion of the agency or judge assessing the final penalty.

\textsuperscript{49} ITAR §§ 127.2(a) and 127.12(a)
\textsuperscript{50} EAR § 766, Supplement No. 1
CHAPTER 4: INTERSECTION OF EXPORT CONTROLS AND UNIVERSITY ACTIVITIES

University Activities Excluded From or Not Subject to Export Control

The EAR, ITAR and sanctions regulations specifically exclude or exempt certain types of information and data from the scope of regulatory oversight. Many of these carve-outs are directly applicable to University research and instructional activities. Although the specific terminology varies among the regulations, they generally exclude information that is published or provided in catalog listed courses. Most university research and academic activities fall within these exclusions and are therefore not subject to export control; however, some university activities are NOT covered by these exclusions. The exclusions that most often apply to university activities are covered in the following paragraphs, while university activities that ARE subject to export control are covered in the following section.

Publicly Available (EAR); Public Domain (ITAR); or Information and Informational Materials (OFAC)

“Information and Informational Materials” are generally excluded from the licensing requirements of most, if not all, of the OFAC country sanctions. The exclusion applies to “publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.”

The EAR contain an exclusion similar to OFAC’s provision in § 734.3(b)(2). However, the EAR go on to exclude additional items as not subject to the EAR because they are publicly available technology and software. Publicly available technology and software includes those items that are already published or will be published; arise during, or result from, fundamental research; are educational; or are included in certain patent applications. These subcategories of publicly available technology and software are further described in §§ 734.7, 734.8, 734.9 and 734.10, respectively (http://www.bis.doc.gov/index.php/forms-documents/doc_view/412-part-734-scope-of-the-export-administration-regulations).

In general, 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 for free or at cost;
- readily available at libraries open to the public or university libraries;
- patents and open patent applications available at any patent office; or

---

51 Similarly, but not identically, defined in each country-specific sanction regulation issued by OFAC; the specific quote provided in the text of this paragraph is taken from the Iranian Transaction Regulations (31 CFR Part 560.315).

52 Prerecorded phonograph records reproducing in whole or in part, the content of printed books, pamphlets, and miscellaneous publications, including newspapers and periodicals; printed books, pamphlets, and miscellaneous publications including bound newspapers and periodicals; children’s picture and painting books; newspaper and periodicals, unbound, excluding waste; music books; sheet music; calendars and calendar blocks, paper; maps, hydrographical charts, atlases, gazetteers, globe covers, and globes (terrestrial and celestial); exposed and developed microfilm reproducing, in whole or in part, the content of any of the above; exposed and developed motion picture film and soundtrack; and advertising printed matter exclusively related thereto.

53 EAR § 734.3(b)(3)
- release at an open conference, meeting, seminar, trade show, or other gathering open to the public.

Fundamental research and educational information are discussed in more detail, below.

As discussed previously in this manual, the ITAR control the export of defense articles, which by definition includes any technical data designated in in the USML. Information in the “public domain” is excluded from the scope of control of the ITAR (unless provided as part of a defense service) by its exclusion from the definition of technical data54. In the ITAR “public domain” means “information which is published and which is generally accessible or available to the public”55. The definition provides a list of ways information may be considered generally accessible or available to the public, including:

- Through sales at newsstands and bookstores;
- Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
- Through second class mailing privileges granted by the U.S. Government;
- At libraries open to the public or from which the public can obtain documents;
- Through patents available at any patent office;
- Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;
- Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency;
- Through fundamental research (see discussion below)

Interestingly, the ITAR do not currently recognize publication via electronic means (i.e. internet) other than through public release following agency approval.

Also of note is the fact that only information released at conferences, meetings, etc. occurring “in the United States” are eligible to be considered to be in the public domain.

**Fundamental Research (EAR & ITAR)**

During the early and mid-1980’s the Federal government and several universities worked together to establish national policy related to the control of information generated in Federally-funded research at colleges, universities and laboratories. This work resulted in the issuance of National Security Decision Directive (NSDD) 189, National Policy on the Transfer of Scientific, Technical and Engineering Information on 21 September 1985. In the wake of the September 11th terrorist attacks, NSDD 189 was reaffirmed in a letter from Condoleezza Rice, Assistant to the President (George W. Bush) for National

---

54 ITAR § 120.10
55 ITAR § 120.11
At the core of NSDD 189 is the following definition of fundamental research:

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

Since the issuance of NSDD 189 in 1985 universities have used this definition to guide their licensing decisions relative to the exclusions provided under the EAR and ITAR.

The “fundamental research” definition in the EAR\(^{56}\) is consistent with that in NSDD 189. Publicly available technology and software that arises during, or results from, fundamental research is excluded from the scope of the EAR’s regulatory authority\(^{57}\). Under the EAR, the results of fundamental research are excluded from the scope of the EAR regardless of whether or not they are published.

The ITAR includes “fundamental research” within the definition of public domain\(^{58}\) (see prior section) and therefore the resulting information will fall outside the scope of regulation, except when provided as part of a defense service. University research will not be considered fundamental under the ITAR if the University or its researchers accept other restrictions on publication of the resulting scientific and technical information; or the research is funded by the U.S. Government and specific access and dissemination controls apply to the results.

Although the definition of fundamental research in the ITAR varies slightly from that expressed in NSDD 189 it has essentially the same meaning. However, given the placement of the definition within “public domain” and its express limitation to “information which is published and which is generally accessible to the public” unpublished fundamental research results may not be considered to be in the public domain unless approved for unlimited public release by the cognizant U.S. government agency\(^{59}\).

Another major difference between how the ITAR and EAR address fundamental research is that the ITAR restricts it to performance at “accredited institutions of higher learning in the United States”. Under the EAR fundamental research it may occur at facilities other than U.S. universities. However, only university fundamental research is restricted to performance within the United States.

**Educational Information (EAR) and General Principles in Science and Engineering (ITAR)**

EAR § 734.3(b) identifies specific items which are not subject to the EAR, including publicly available technology and software that are “educational”. “Educational information” is not subject to the EAR if it is “released by instruction in catalog courses and associated teaching laboratories of academic

---

\(^{56}\) EAR § 734.8  
\(^{57}\) EAR § 734.3(b)(3)(ii)  
\(^{58}\) ITAR § 120.11  
\(^{59}\) ITAR § 120.11(a)(7)
institutions.” It is important to note that this exclusion does not apply to mentoring and instruction provided outside of the classroom, e.g. to students performing research.

The ITAR controls defense articles, which by definition includes technical data designated on the USML. However, “information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities” is specifically excluded from the definition of technical data under the ITAR.

The following is one example of how these definitions apply to university activities. The university offers a catalog listed course in very high-speed integrated circuit design and manufacturing. The course is open to any University student who has completed the necessary prerequisite courses. In this case the material presented in the class will not be subject to export controls despite the fact that very high-speed integrated circuits are on the CCL. The key factors here are that the information is provided in a catalog listed course and the course is open to any qualified individuals regardless of nationality. This is not the case when instruction is related to a defense article subject to the ITAR (see “Defense Services” in Educational/Training Situations on page 32).

Areas of Continuing Impact on Academic Pursuits and Activities

Physical Export of Items, Including Technical Data, or Technology

The University may ship equipment, machinery or supplies abroad for a variety of purposes; including participating in a conference or other meeting, to conduct research, to participate in a collaborative or joint program, or to loan equipment to another institution.

The physical shipment of items abroad is an export from the U.S. The purpose of the shipment (i.e. to conduct fundamental research or to provide academic instruction) is irrelevant in determining whether or not it is subject to control under the export regulations. Both the USML and CCL are lists of items and technologies not the intended use. Licensing requirements are the same for commercial exports and those conducted in support of University activities. That said, the applicability of certain license exceptions or exemptions may be impacted by the purpose and duration of the export.

When no license exception or exemption is available to cover a proposed export and the recipient foreign party is otherwise eligible to receive the intended export, the Office of Export Controls will apply for export authorization from the appropriate U.S. Government agency (BIS, DDTC or OFAC). No export will occur unless and until agency approval is granted and the University has confirmed with the individuals involved that they can and will apply with all provisos and conditions associated with use of the license or other authorization.

---

60 EAR § 734.9
61 ITAR § 120.6
62 ITAR § 120.10
“Deemed” Exports and Technical Data Exports in the U.S.

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). Both the ITAR and the EAR provide for deemed exports, even though in the case of defense exports the term “deemed export” is not used in the regulations. While the ITAR distinguishes between the transfer of technical data and providing a defense service in the definition of “export,” the EAR generally provides for the release of technology. Such transfer or release may be made through oral, visual, or other means. The following are examples of how an export may occur:

1. allowing virtual or physical access*;
2. a demonstration, briefing or presentation;
3. a conversation (in-person or telephone);
4. laboratory or plant visit;
5. faxes or letters;
6. hand-carried documents, hardware or drawings;
7. design reviews;
8. the exchange of electronic data or communication;
9. posting non-public data on the Internet or the Intranet;
10. carrying a laptop or other electronic device with controlled technical information or software to an overseas destination; or
11. collaborating with other universities / research centers through research efforts.

*The EAR and ITAR differ in controls related to access. Under the ITAR providing a foreign national the ability to touch, see or use a defense article would be an export if such access provides technical data, while under the EAR it would only be an export if it released technology or software subject to the EAR as described in 734.2(b)(2). Note, however, that foreign national licensing guidance provides that any “access” by a foreign person to a defense article would require a license. [In the event an unlicensed foreign person had unrestricted access to a defense article, it would be difficult, if not impossible, to show that the foreign national did not obtain technical data by deconstructing, examining or reverse engineering the defense article.]

The issue of deemed exports is particularly relevant to university research because of the activities that normally take place at a university, largely, teaching and research. Whenever teaching or research activities are related to controlled equipment or technology, the involvement of foreign students or researchers may trigger export control compliance issues.

As with physical exports, most transfers of technical information at universities do not require a license. One reason for this is that technology controls do not apply to many of the items on the CCL. A second

63 ITAR § 120.17(a)(3-5) and EAR § 734.2(b)(1)
64 EAR § 734.2(b)(2)(ii)
65 ITAR § 120.17(a)(4) addresses technical data transfers; ITAR § 120.17(a)(5) covers provision of defense services.
reason is that access to controlled (as identified on the CCL) “development” or “production” or “use” technology is rarely required to conduct university activities. Although it may seem likely that universities would frequently need to transfer “use” technology to foreign nationals, the fact that the definition of “use” involves more information than would normally be available in an operation or owner’s manual\(^\text{66}\) actually makes exports of “use” technology relatively infrequent. Even when a license requirement does exist based on the specific ECCN and Country Chart\(^\text{67}\), a license exception may be available to overcome the license requirement for the proposed deemed export.

The ITAR provides one broad license exemption specifically for universities which may be useful for some projects; this is often referred to as the Bona Fide Employee Exemption (BFEE)\(^\text{68}\). This exemption permits disclosures of unclassified technical data in the U.S. by U.S. institutions of higher learning to foreign persons who are their “bona fide and full time regular employees” when certain criteria are met. This exemption may not be used for employees who are nationals of a country to which exports of defense articles and services are prohibited\(^\text{69}\). The BFEE may be used for nationals of other countries provided the employee resides in the U.S. throughout the period of employment\(^\text{70}\) and the university informs the foreign national in writing that the technical data may not be transferred to other foreign nationals without the prior written approval of DDTC. It is important to note that this license exemption is not available for students, trainees, collaborators, consultants, or individuals who are not both full time and regular employees of the university.

“Defense Services” in Educational/Training Situations

As mentioned previously, the ITAR differentiates between the export of technical data to a foreign person in the U.S. and the provision of defense services. While the BFEE may be used to permit the University to share an ITAR-controlled blueprint or technical specification document, it does NOT allow a U.S. person to provide instruction or consultation related to the information contained in the document. Likewise, the BFEE does not permit a U.S. person to demonstrate or provide instruction in the operation of a defense article. Such activities are considered defense services\(^\text{71}\) and would require specific authorization from DDTC. It is important to note that a defense service can be performed even when the information provided is already in the public domain; this is made clear by the following statement:

“… The requirements of this section apply whether or not technical data is to be disclosed or used in the performance of the defense services described in §120.9(a) of

\(^{66}\) EAR § 772 defines “use” to include all of the following six elements “operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing”. Note that for “600 series” items on the CCL, only one element may be necessary to constitute “use”.  
\(^{67}\) EAR § 738, Supplement No. 1  
\(^{68}\) ITAR § 125.4(b)(10)  
\(^{69}\) ITAR § 126.1  
\(^{70}\) Email clarification from Charles Shotwell, Office of Defense Trade Controls Policy, to the University of Oklahoma. 16 December 2011. In summary, the email states that the term “permanent abode” used in 125.4(b)(10) was intended to mean “residence” and that the wording of the visa is not necessarily determinative.  
\(^{71}\) ITAR § 120.9
This statement is taken from the section of the ITAR that addresses manufacturing license agreements (MLA) and technical assistance agreements (TAA). In the absence of some other applicable exemption, the University would have to obtain authorization (typically in the form of an approved TAA rather than an MLA for University activities) from DDTC before providing a defense services to a foreign national, whether or not an employee.

Therefore, although “information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities and information in the public domain” are not “technical data” and do not require a license for export, providing the same information in relation to a defense article is a defense service and would require prior approval by DDTC. There is no exclusion or exemption available to cover such exchanges when they occur in the context of a university course or fundamental research activity.

When no license exception or exemption is available to cover a proposed deemed export, technical data transfer, or defense service, and the recipient foreign party is otherwise eligible to receive the intended export, the Office of Export Controls will apply for export authorization from the appropriate U.S. Government agency (BIS, DDTC or OFAC). No export will occur unless and until agency approval is granted and the University has confirmed with the individuals involved that they can and will apply with all provisos and conditions associated with use of the license or other authorization.

---

72 ITAR § 124.1
73 ITAR § 120.10 definition of technical data
74 ITAR § 124.1(a) Manufacturing license agreements and technical assistance agreements, Approval.
CHAPTER 5: UNIVERSITY OF VIRGINIA EXPORT CONTROL POLICY & RESPONSIBLE PARTIES

Institutional Commitment

The University of Virginia conducts research to advance knowledge, engage students, enhance learning, and build its reputation in the scientific and technical communities by providing excellent return for investment on sponsored awards. The participation of students in research activities is central to the University mission. The research activities conducted at the University of Virginia are overwhelmingly fundamental in nature, including both basic and applied activities. The University does not normally accept restrictions on the publication of research results or participation of foreign nationals in the conduct of the research. In rare cases, exceptions may be made to permit externally funded research with limits on publication or foreign national restrictions, of which are export controls are one example. Each request to accept restrictions will be reviewed on its own merits. Among the factors that will be considered in determining whether a particular activity is acceptable to the University are the following:

- the academic merit of the proposed activity;
- the compatibility of the proposed activity with the mission of the University;
- the nature of the restrictions; and
- the contribution of the activity to the benefit of humanity.

The University of Virginia has formalized its commitment to compliance with U.S. control laws and regulations through the adoption of Financial Policy #043 (FIN-043) on November 29, 2011, with the most recent revision published in February of 2016. This policy sets forth both institutional expectations for compliance and identifies the institutional executives and offices responsible for oversight and administration. The current policy can be found in Appendix I of this document or may be accessed electronically through the University’s publicly available Policy Directory (http://uvapolicy.virginia.edu/policy/FIN-043).

Empowered Officials

The following individuals have been designated as “Empowered Officials” pursuant to the University’s ITAR registration with DDTC:

- Executive Vice President and Chief Operating Officer,
- Director, Finance Outreach and Compliance
- Export Compliance Officer

These individuals also have the authority to seek export authorizations from BIS and OFAC in support of University activities. Each of the “Empowered Officials” listed above also have the authority to stop any export that may be in violation of U.S. export control regulations and when necessary to submit voluntary disclosures to the appropriate regulatory agency (ies) on behalf of the University.
The role of the **Office of Export Controls** is to facilitate the University’s research, teaching, service and patient care mission by administering a program to support this policy; to that end, the Office of Export Controls is responsible for:

- Establishing and administering procedures, forms, and processes to facilitate compliance with this policy;
- Developing and delivering outreach and training materials for University faculty, staff, students and trainees to increase export control awareness;
- Performing restricted party screening, as requested, for persons or entities with which the University will be conducting business or collaborating, including sponsors, collaborators, foreign national employees, visiting scientists or scholars, subrecipients, and subcontractors;
- Providing tools to the University community to assist in the identification and management of export control issues;
- Working with faculty members to develop Technology Control Plans, including IT security measures, and granting final written approval for these Plans;
- Performing all requested I-129 certification reviews for the University within 2 business days of the initial request and providing the requisite certification letters;
- Performing all requested export licensing assessments for international shipments;
- Conducting assessments, as requested, for international travel;
- Managing the University’s export control related registrations and online accounts with regulatory agencies;
- Advising Authorized Institutional Signatories on export control issues related to contracts (*FIN-036*) and academic program agreements (*FIN-035*);
- Seeking export authorizations and clarifications on behalf of the institution as necessary and appropriate to support University activities; and
- Performing compliance monitoring and risk assessment activities.

The **Director of Finance Outreach and Compliance** is responsible for:

- Providing general oversight of the export controls function (Office of Export Controls) and the direct supervision of the Office of Export Controls staff;
- Acting as the University’s secondary or additional point of contact for agencies with regulatory or enforcement authority under the Regulations;
- Serving as an Empowered Official of the University, as defined in the International Traffic in Arms Regulations (22 CFR 120.25), with the independent authority granted by the University in all matters governing foreign trade, export administration, export compliance oversight, investigations, and to stop any transaction or to refuse approval for any action that is deemed not to be in full compliance with the Regulations or University policies governing such action or transaction; and
- Signing and submitting export control and compliance related documents, including, but not limited to, license applications, voluntary disclosures, commodity jurisdiction requests, requests for advisory opinions, export certifications and other export related requests for approval to Federal agencies and other parties in behalf of the University.
The Export Compliance Officer is responsible for:

- Serving as the University’s principal point of contact for agencies with regulatory or enforcement authority under the U.S. export control regulations;
- Establishing, and revising when necessary, the programmatic framework through which the University manages export controlled activities at the University, including development and dissemination of policies, procedures, educational materials and website content; Serving as an Empowered Official of the University, as that term is defined in the International Traffic in Arms (22 CFR 120.25), with the independent authority granted by the University in all matters governing foreign trade, export administration, export compliance oversight, investigations, and to stop any trade transaction or to refuse approval for any action that is deemed not to be in full compliance with the Regulations or University policies governing such action;
- Signing and submitting export control and compliance related documents, including, but not limited to, license applications, voluntary disclosures, commodity jurisdiction requests, requests for advisory opinions, export certifications and other export related requests for approval to Federal agencies and other parties in behalf of the University;
- Investigating potential export control violations related to the conduct of University activities;
- Providing outreach, assistance, and training to University faculty, staff, students and trainees regarding the laws, regulations, and University procedures associated with export control; and
- Performing periodic risk assessments to evaluate the relative strengths and weaknesses of the University’s export compliance program and providing the assessment results to the Vice President for Finance and to the Executive Vice President and Chief Operating Officer for their review and action, if appropriate.

Broadly speaking the role of the Office of Export Controls (OEC) is to serve as central resource for export control information and to coordinate the overall export compliance management program for the University. The Key University Offices & Roles listed in the following section are those that together with the OEC are central to assuring institutional compliance with U.S. export controls.

Key Cooperating Offices & Roles

Office of Sponsored Programs

The Office of Sponsored Programs (OSP) assists OEC with the identification of export control risks in proposals, funding award terms and conditions, and other sponsored research agreements including, but not limited to, nondisclosure agreements, licensing agreements and material transfer agreements. OSP personnel are offered training and checklists to help them identify possible export control risks and know when to route it to OEC for additional review.
Office of the Vice Provost for Research

The Office of the Vice President for Research has the final authority to determine whether or not the University of Virginia will accept research restrictions including those associated with export controls. The University’s organizational structure is such that all researchers ultimately report to the VPR. The VPR’s office assists OEC with outreach and is involved with all inquiries related to suspected non-compliance with University policy or export control regulations.

Procurement & Supplier Diversity Services

University purchasing or procurement functions are managed by Procurement & Supplier Diversity Services (PSDS). PSDS assists with the University’s export control program by screening new vendors and requesting export control information from vendors when they are acquiring technology; this is typically for purchases valued at $5000 or more. Smaller purchases may be made by research or departmental personnel using a Purchase Order in the UVA Marketplace or a University Procurement Card (P-Card). All P-Card users are provided basic information on export controls and reminded of their responsibility to ensure that vendors provide notification to the Office of Export Controls before providing defense articles to the University on an annual basis. PSDS also includes within the University’s standard terms and conditions for all vendors, that vendors provide written notice via email, and receive prior written authorization from the Office of Export Controls, before delivery to the University, for any items it will be providing to the University that are controlled under the International Traffic in Arms Regulations. See http://www.procurement.virginia.edu/pagepterms. The University’s Surplus Property Program is managed by PSDS. Information on the Surplus Property Program may be accessed at http://www.procurement.virginia.edu/pagesurplushome.

Human Resources

The Compliance and Immigration Services (CIS) group within Human Resources manages visa applications, including modifications and renewals, for institutionally sponsored employees. Although most foreign national University employees are in the U.S. on H1B visas there are a small numbers holding other visa types. CIS files all I-129 (Petition for a Nonimmigrant Worker) applications on behalf of the University but requires each sponsoring department or supervisor to include an Advisory Letter from OEC stating the appropriate response to Part 6 (Certification Regarding the Release of Controlled Technology or Technical Data to Foreign Persons in the United States). In order for OEC to perform the necessary review, the sponsoring department or supervisor must complete the University’s I-129 Export Certification Request Form and submit it to OEC for review. The University’s Office of Compliance and Immigration Services has instructions contained in the H-1B Packet available on this page: http://www.hr.virginia.edu/other-hr-services/CIS/immigration-services/immigration-packets/. The Office of Export Controls has additional information provided on its website here: http://export.virginia.edu/i-129-export-certification.
Office of the Comptroller

The Director of Tax Compliance & Operational Contracts serves as institutional signatory on Academic Agreements not involving sponsored research and ensures that all proposed agreements and foreign parties are screened by OEC prior to executing the final contract.

International Studies Office

The International Studies Office (ISO) manages visa applications for students and scholars. The International Students and Scholars Program staff in ISO provide programming and services to support the adjustment and integration of international students and scholars the U.S. and the university community. ISO provides OEC with citizenship and immigration status for foreign national students and scholars proposed for addition to export controlled projects or programs.

Faculty Members

Faculty members 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, and with fellow researchers or collaborators. As set forth in the University’s export control policy all faculty members share the following export control responsibilities:

- Consulting with and providing assistance to the Office of Export Controls to ensure that controlled technology, regardless of whether it is instructional or research technology, used or produced by them or under their supervision is categorized and safeguarded correctly under U.S. export control regulations;
- Knowing and complying with the terms and conditions of their funding awards and other agreements, including export controls, limitations on publication of research data and results and any foreign national restrictions;
- Assisting the University in preventing unauthorized exports and applying for government licenses where appropriate;
- When applicable, developing a technology control plan, receiving export controls training, submitting the plan for approval, and following the requirements of the approved plan;
- Seeking advice from the Office of Export Controls as necessary; and
- Ensuring that staff, students, trainees and foreign visitors under their supervision are made aware of any applicable requirements and/or restrictions (e.g., university, regulatory, or sponsor imposed) and that they receive adequate training in how to conduct their activities in compliance with those requirements.
University Personnel

According to the University’s export control policy all employees, trainees and students, regardless of whether or not assigned to an export control project or program, have the following export control responsibilities:

- Knowing and complying with any legal, regulatory or University requirements applicable to their activities;
- Seeking assistance from the Office of Export Controls prior to performing any export, including deemed exports, of technology, software or goods; and
- Reporting any suspected non-compliance with U.S. export control regulations or this policy to the Office of Export Controls.

Office of the General Counsel

The University General Counsel has appointed an Associate Counsel to advise the Office of Export Controls on legal matters. In addition, all requests for outside counsel must be approved by the Office of the General Counsel prior to going to the Attorney General’s Office of the Commonwealth of Virginia for final approval and appointment.

Export Controls Advisory Committee

The Export Controls Advisory Committee (ECAC) is an ad hoc committee that provides input to the OEC Director on elements of the Export Control Management Program (ECMP) that impact their areas of responsibility and assist with the dissemination of ECMP information to the University community. The OEC will also request that the ECAC provide an assessment of the factors that contributed to an incident of non-compliance with University policy and procedures or violation of U.S. export controls and recommend a course of action to prevent similar incidents in the future. The ECAC membership is comprised of representatives from each of the Key University Offices listed above.
Note: Boxes with gray background indicate the Key Cooperating Offices & Roles identified in the Organizational chart. The boxes outlined in red indicate the individuals who are empowered to apply for export licenses and other authorizations on behalf of the University.
CHAPTER 6: UNIVERSITY OF VIRGINIA PROCESSES & PROCEDURES

Export Control Analysis of Research Projects/Programs

Purpose: The pre-award staff of the Office of Sponsored Programs (OSP) review sponsored research project proposals, grants, contracts and other contractual arrangements relating to sponsored research for potential export control issues of concern. The Office of Export Controls (OEC) reviews all projects that are forwarded by pre-award staff after their initial review.

Initial Review

The pre-award staff in the Office of Sponsored Programs may perform an initial review by using the Export Control Checklist, see Appendix II, as a resource. The reviewer will look for the following red flags indicating potential export control issues:

- References to U.S. export control regulations, beyond a simple statement that parties must comply with applicable U.S. laws and regulations;

- Restrictions on publication or dissemination of research results, including but not limited to, prior approval by the sponsor;

- Assertions that project results will be proprietary or trade secret;

- restrictions on access or participation based on citizenship or nationality;

- involvement of foreign sponsors or collaborators, other than foreign national employees of U.S. persons;

- funding, direct or indirect via subcontract, from the “high risk sponsors”, examples include the following:
  - Department of Defense, including all agencies, labs, and branches of the armed services;
  - Department of Energy;
  - Department of Homeland Security;
  - National Aeronautics and Space Administration; or
  - Intelligence Agencies

- military applications of the project results; or

- international travel, shipping, or performance sites.
If the reviewer finds any possible “red flags” they should mark the file as requiring further review by the Office of Export Controls and forward all relevant information to OEC prior to final execution of the agreement or acceptance of the award.

**Office of Export Control Review**

- DOD, DOE, Intelligence Agency or NASA funded projects should have the export control checklist completed.

- If there is already a checklist accompanying a project agreement delivered to OEC for review, review the checklist for any red flags that OSP pre-award has identified. Investigate the identified red flags for export control issues.

- After reviewing the checklist, or if there is no checklist but the file was forwarded to OEC for review anyway, the project file itself should be investigated for export control issues.
  - Examine the terms.
    - Are there any references to export controls, including restrictions on participation by foreign nationals?
    - Are there any publication or dissemination restrictions that could make the use of the Fundamental Research exemption problematic?
    - On DOD funded projects, is the DFAR 252.204-7012 clause delineated?
  - Examine the proposal budget.
    - Are there any expenses for foreign travel included?
    - Are there expenses for equipment that could potentially be export controlled?
  - Examine the project statement of work.
    - Look for any references to collaborations with parties in foreign countries, or with foreign nationals domestically.
    - Are there any plans to ship equipment internationally in association with the project?
    - Will any of the research involve any components of any military hardware?
    - Will the research involve armor materials?
    - Will the research involve energetic materials?
    - Will the research involve any pathogenic compounds?
• If restrictions on publication or dissemination are included in the terms, the OPS pre-award staff must have authorization from the principal investigator indicating their willingness to accept and abide by the restriction. Approval must also be sought from the principal investigator’s department chair, dean’s office, and the Office of the Vice Provost for Research.

• If the DFAR 252.204-7012 clause is present, ensure that the principal investigator is aware of the obligation to follow the standards for IT security and safeguarding covered defense information demanded by the clause.

• If foreign travel is indicated, review with the principal investigator what their responsibilities are as an employee traveling internationally on University business.

• If any work with potentially export controlled materials, technical data or technology is indicated or anticipated, investigate the materials to determine its export control classification. If the establishment of a Technology Control Plan (TCP) is necessary, work with the principal investigator to ensure that the TCP is in place as soon as possible (preferably before the export controlled materials arrive on Grounds.)

**Export Control Analysis of International Academic Agreements**

All academic agreements with foreign institutions will be reviewed by the Office of Export Controls to ensure they do not involve restricted parties or export controlled activities, including the provision of defense services or assistance to foreign atomic energy activities. If exports are required to support academic agreements, the OEC will work with the involved UVA department and personnel to assure that any required export authorizations are obtained and the use of any license exception or exemption is documented.

**Assessment: Identification, Marking and Tracking of Listed Materials**

Purpose: There are many inventions and innovations generated at the University. These materials should be assessed for export control status and classification. Records of the assessment process must be kept.

*University Developed Items, Including Technical Data (ITAR) or Technology (EAR)*

• The first step should be to determine which export regulation (EAR or ITAR) applies to newly invented items and technologies.
To determine if an item is controlled under the ITAR or EAR, the evaluator should work to determine ITAR applicability first, as the regulations are much narrower in scope. The evaluator should ask the following questions to determine ITAR applicability.

- Was the item produced as part of a sponsored project funded by a DOD grant or contract?
- Does the item have an obvious military application (such as munitions or armor?)
- Was the item designed to be incorporated into already existing military hardware or information systems?
- Was the item specifically designed, developed, configured, adapted, or modified for a military application?
- Can the item be described as being a Firearm, Munition, Explosives, Vessels of War or Naval Equipment, Military Vehicle, Aircraft, Military Training Equipment, Personnel Protective Equipment, Military Electronics or Software, Radar and other Guidance and Control Equipment, or an Infrared Camera?

If the answer to any of the previous five questions is yes, then a detailed evaluation should be performed to determine if the item is included on the ITAR.

If the detailed evaluation of the item fails to definitively categorize the item, then OEC will seek guidance from the Department of State Directorate of Defense Trade Controls via a Commodity Jurisdiction.

If the answer to all the questions is no, then the item should be considered subject to the EAR and should be further evaluated to determine the ECCN.

- If the item is deemed to be subject to the EAR, it shall be the responsibility of the OEC and the PI to determine the ECCN of the item in question.

- The evaluator should work closely with the PI to determine the ECCN through a process of elimination of relevant ECCN’s.

- The evaluator should consult the Commerce Control List Index, which can be found at http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear. The CCL index gives simple, layman’s terms titles to the wide variety of items listed on the CCL and is a good place to find the section of the CCL that pertains to the product.

- If the CCL index does not point the evaluator in the right direction, the EAR features a guide to self-classifying called the Commerce Control List order of review. The evaluator should follow the steps delineated in Supplement No. 4 to Part 774 of the EAR to determine the ECCN. If no appropriate ECCN is found, classify the product as EAR99.
If doubt exists regarding the correct classification of an item or technology, the OEC shall confirm the self determination by requesting a Commodity Classification from BIS.

- Note that items and technical data, not including the results of fundamental research, which are developed specifically for a military use will be treated as ITAR until designated as subject to the EAR by DDTC (i.e. in response to a Commodity Jurisdiction request).

- Also note that the results of unrestricted fundamental research, whether or not externally sponsored, will not be subject to a Technology Assessment until one of the following occurs.

  - There is a need to physically export an item developed by UVA in the conduct of fundamental research; or

  - The UVA Patent Foundation (PF) determines there is commercialization potential and directs that the invention (item and associated technical data) or innovative technology be protected as proprietary or trade secret.

- Records regarding technology assessment and identification conducted by the OEC will be kept and maintained by the OEC.

### Outgoing International Shipments

Purpose: University personnel are responsible for contacting the Office of Export Controls (OEC) for a technology and export control assessment prior to exporting any item out of the U.S. The OEC can assist University exporters with determining if any export regulations apply to their shipment, outlining the proper course of action to assure compliance, and applying for government authorizations if necessary.

- The first step should be to determine the export control classification of the item to be exported, as the regulatory requirements of the shipment cannot be determined without knowing the classification of the item.

  - The reviewer should decide whether self-classification or contacting the manufacturer for a classification would be the most prudent course of action. For example, almost all medical devices and supplies are classified as EAR99, so, depending on the item being reviewed, it may not be a worthwhile endeavor to seek a classification from the manufacturer.

    - If self-classifying, please refer to the section on assessment for guidance.
• Reviewers may contact the manufacturer of the item in question to obtain the classification.
  - The reviewer should attempt to contact whoever at the company has export control responsibility. These people frequently can be found in the logistics or legal departments.
  - Some manufacturers publish their export control classifications on their websites, particularly in the tech industry.
  - Reviewers should be prepared to encounter apathy and occasionally outright resistance from manufacturers when requesting classifications.

• After the classification of the item has been established, the reviewer must determine if the item can be exported to the destination without government permissions.
  - If the item is classified as controlled under the ITAR, the reviewer should anticipate having to apply to DDTC for an export license, which would delay the shipment significantly as the wait for approval can be lengthy.
  - If the item is to be sent to Cuba, Iran, North Korea, Sudan, or Syria the Office of Export Controls must be contacted by the shipper. Although there are exceptions, these countries are subject to comprehensive embargoes and it is unlikely a shipment would be allowed to these countries without a specific authorization from OFAC.
  - If the item is determined to be controlled under the EAR, the reviewer must examine the ECCN and determine its specific requirements for the destination country.
  - It is a best practice to perform a restricted party screening on all individuals and organizations that will serve as shipment consignee.
  - The reviewer should then ask the following questions:
    - Do General Prohibitions 4-10 apply? (see 736.2(b)(4-10))
      - If yes, seek a license from the BIS, if no, move on to the next question.
    - Are there reasons for control in effect? Consult the country chart (Supplement No. 1 to Part 738 of the EAR) to determine if the ECCN’s stated reasons for control apply to the destination country.
• If no, the shipment is deemed “no license required” and the shipment can go ahead without further evaluation. If yes, move on to the next question.

• Is a license exception available? (See part 740 of the EAR)

• If yes, use the license exception and ship the product. OEC should instruct the shipper on the proper use of a license exception, and offer the use of the University AES account to ensure accurate filing.

• If no, then a license is required. The OEC will apply for the required license on behalf of the University shipper.

• After the export evaluation is completed, the OEC will advise the shipper of the steps required to ensure compliance.

Procurement Activities

Whenever possible the University prefers to rely on manufacturers to provide the export control status of items and software being obtained through a procurement activity. Purchasers within Procurement and Supplier Diversity Services handle all procurements valued at ≥ $5000 or requiring a contract with the University; smaller value purchases are handled by purchasers in research, academic, or support offices.

The University’s standard vendor contract now includes a term requiring vendors to notify the Office of Export Controls (OEC) and receive written authorization from OEC prior to delivering any defense article to the University. University purchasers are instructed to require all vendors, whether or not contracted, to identify defense articles prior to delivery. Purchasers are should request the ECCN or USML category for any items they are procuring if they have reason to believe the items will be subsequently exported.

In cases where the vendor does not know the export control status of an item (e.g. when the vendor is not the manufacturer) or refuses to provide export control information to the University, the Office of Export Controls will perform a self-determination based on the available information. In cases where doubt exists as to the jurisdiction of the item(s), the University will either decline to purchase or will proceed with the purchase and protect the item as a defense article until it is conclusively shown to be subject to the EAR (e.g. through a formal response to a commodity jurisdiction or advisory opinion request).

Purchases valued at <$5000 may be made by using a UVA Travel and Expense Card if otherwise eligible under institutional policy and procedures. All individuals issued a Travel and Expense Card are required to complete initial and annual refresher training; this training informs them of their responsibility to
request export control information from vendors prior to placing an order and to notify the Office of Export Controls prior to proceeding with the purchase of any ITAR controlled items (defense articles).

**Surplus of University Property**

All surplus of University property must comply with Surplus Property Disposal policy (X.F.1) and associated procedures issued by Procurement and Supplier Diversity Services (http://www.procurement.virginia.edu/pagesurplusprocedure). The University surplus procedures are compliant with the general principles expressed by BIS in their advisory opinion on public sales in the US; no ITAR controlled items may be surplussed without the express authorization of the Office of Export Controls. University surplus may not be exported, directly or indirectly (i.e. provided to an individual or entity when there is reason to believe that it will subsequently be exported), without the authorization of the Office of Export Controls.

**Other Agreements for Incoming Items, Including Technical Data (ITAR) or Technology (EAR)**

The University may acquire materials (intellectual property, equipment loans, biological materials, software, etc.) from other parties in a variety of ways other than through a purchase or procurement activity, the following are examples:

- **Sponsored Agreements** – some funding awards may include access to or the loan of items by the sponsor or other party to the agreement in order for the University to conduct its defined scope of work. Such arrangements are reviewed and negotiated by UVA Office of Sponsored Programs pre-award staff as described previously (see Export Control Analysis of Research Projects/Programs).

- **Material Transfer Agreements** – typically used for the transfer of biological specimens, these agreements are reviewed and negotiated by University contract negotiators in the Office of Sponsored Programs or the Office of Grants and Contracts at the School of Medicine. Although MTA’s may not be associated with a Sponsored Agreement, they are reviewed similarly for export control issues but with particular attention focused on identifying select agents and export controlled biologics or toxins.

- **License Agreements** – Institutional license agreements are subject to the same review process as indicated in the previous section, Procurement Activities, although the terms and conditions are negotiated by University contract negotiators. The OEC will be responsible for

---

corresponding with the University contract negotiator and vendor regarding export control language and terms in the license agreement.

- Nondisclosure or Confidentiality Agreements – used for the exchange of protected personal (e.g. under HIPAA\textsuperscript{76} or FERPA\textsuperscript{77}), proprietary or U.S. government restricted information; typically information will be provided in the form of oral disclosure or documents (hard copy or electronic) rather than items or materials. Such arrangements are reviewed and negotiated by UVA pre-award staff in the Office of Sponsored Programs as described previously (see Export Control Analysis of Research Projects/Programs).

- Donations – Occasionally the University receives donations of equipment or other material, these donations will be subjected to the same review process as described for Procurement Activities, above.

- Equipment Loans, other than as part of a Sponsored Award – are subject to the same review process as indicated in the previous section, Procurement Activities. In fact equipment loans that are not part of a Sponsored Award must be submitted as zero dollar purchase orders to ensure proper negotiation, marking, protection, insurance, and return of loaned equipment.

Restricted Party Screening

Purpose: To determine if any interactions with international entities or individuals could be in violation of current US restrictions on dealings with certain parties, and more generally to exercise due diligence and best practices. To this end, the University maintains a license with eCustoms for the use of Visual Compliance, which is a web-based screening service. It screens user entries against all government denied and restricted party lists (including those related to export control), as well as several other useful services. Visual Compliance can be provided to anyone on grounds with a need for the service at no charge, or OEC can perform the check on behalf of anybody on grounds and will provide them with the results.

Restricted party screening will be performed on the following parties:

- All proposed parties to an ITAR controlled project or program;
- All parties initially named in a Technology Control Plan, or proposed for addition later;
- Non-UVA parties to a physical export (e.g. receiving party, end-user, consignee, shipper, freight forwarder, etc.);

\textsuperscript{76} The Health Insurance Portability and Accountability Act of 1996; P.L. 104-191; enacted August 21, 1996. The HIPAA Administrative Simplification Rules are located at 45 CFR Parts 160, 162 and 164.

\textsuperscript{77} The Family Educational Rights and Privacy Act of 1974 (a.k.a. the Buckley Amendment) codified at 20 USC § 1232 with implementing regulations at 34 CFR Parts 99.
• Foreign parties to an international academic agreement;
• Foreign parties to a sponsored award or contract, including subcontractors;
• Parties to a foreign financial transaction;
• Foreign national employees as part of the University’s internal review process for all I-129, Petition for a Nonimmigrant Worker, applications being submitted to the U.S. Customs and Immigration Service. (See related information).
• The consignee on international outgoing shipments;
• Foreign parties (and the organizations they are employed by) visiting UVA in an official capacity should be screened before arriving on grounds.

When screening in Visual Compliance, it is essential that the screener complete the comment section to describe the reason for screening the entity or individual, in simple and consistent terms. Below are a few examples of search reasons to be entered on the comment line.

• I-129 Export Certification
• Outgoing Shipment
• Vendor Review
• SCPS Program Participants

All screenings should be set to Fuzzy Level 2. While this may result in more false positives, it is necessary as many names and organizations are not translated consistently, or may have changed names at some point.

Any “red flags” identified during the restricted party screening must be resolved before proceeding with the planned export. Continuing compliance is an additional feature of the University’s Visual Compliance subscription. This feature includes daily re-screening of all previously screened parties with change notifications being emailed to the person who originally performed the screening as well as the UVA account administrator for Visual Compliance.

Should the status of an individual change such that they are no longer eligible to receive or have access to export controlled items or information or a new licensing requirement becomes applicable, the screened person (individual or entity) will immediately be removed from any TCP or otherwise controlled project, participation in any University export activity will be prohibited, and access to controlled items and information will be removed until a license is obtained, if that is an option under the specific terms of the restriction. Even when an option to apply for a license exists, the University may make a business decision not to pursue a license and to maintain the internal restrictions on participation and access.
Technology Control Plan

Purpose: A Technology Control Plan is the formalization of the processes and procedures the University project personnel will use to ensure that any subject items and information are not disclosed to unauthorized personnel or exported. The Office of Export Controls has created a template TCP (Appendix III) to serve as a starting point, with the intention that it be adapted first and foremost to comply with the specific U.S. regulatory requirements and secondly to accommodate the needs and structure of the University project or program.

TCP Development

It is the responsibility of the Principal Investigator or program leader, who is identified on the TCP as the “Responsible Person”, to develop, manage and enforce compliance with the terms of the TCP. The Office of Export Controls will assist with development and determine whether or not it is sufficient to adequately protect the subject items and information from unauthorized access and export. The TCP will include the following:

1. A commitment to export controls compliance;
2. Identification of the relevant export control categories and controlled technologies;
3. Identification of the project’s sponsor(s);
4. Identification and nationality of each individual participating in the project;
5. Physical and information security measures appropriate to the subject items and information;
6. Personnel screening measures; and
7. Instructions pertaining to disposition of subject items and information (hard copy and electronic) at the end of the project or program.

Security Measures

The physical and information security measures to prevent unauthorized access and export must be included in the TCP. Examples of security measures include, but are not limited to, the following:

- **Compartmentalization.** Project operation may be limited to laboratory areas that are physically shielded from access or observation by unauthorized individuals. Such areas must remain secured at all times when subject items or information are in use.

- **Time Blocking.** Project operation may be restricted to specific time blocks when access will be limited to authorized personnel. Unauthorized individuals shall not be permitted to observe project operations or have access to the space during this time.

- **Marking.** Export controlled information must be clearly identified and marked.
• **Personnel Identification.** Authorized individuals may be required to wear a badge, special card, or similar device indicating their permission to access project areas. Physical movement into and out of designated project area may be logged or otherwise monitored.

• **Secure Storage.**
  - Tangible items should be stored in controlled access rooms or storage devices that prevent visual disclosure as well as physical access. Access keys or cards may only be issued to authorized personnel.
  - Soft and hardcopy data, laboratory notebooks, reports, and other research materials should be stored in locked storage devices. Keys may only be issued to authorized personnel.

• **Electronic Security.**
  - Project computers, networks, and electronic files should be secured and monitored through User IDs, password controls, and encryption technology (128-bit or better). Database access should be managed via a Virtual Private Network.
  - Electronic communications (email, text and instant messaging) containing controlled information should be either explicitly prohibited or specifically addressed in the TCP procedures.

• **Project Communications.** Discussions about the project must be limited to the individuals identified and authorized under the TCP and occur only in areas where unauthorized individuals are not present and cannot reasonably overhear. Discussions with non-UVA parties must occur only under signed agreements which fully respect non-U.S. person limitations for such disclosures.

**Required Training**

Before any individual may have access to items or information controlled and protected under a TCP, he or she must complete the initial training requirement, be informed of the procedures authorized under and receive a copy of the TCP, certify his or her agreement to comply with all security measures contained in the TCP, and be authorized by the Office of Export Controls. Training is provided by the OEC, or if preferable to the parties listed on the TCP, individuals have the option of taking online export controls training offered through CITI (Collaborative Institutional Training Initiative), a commercial vendor which UVA has contracted with to provide various types of compliance training to its faculty, staff and employees. Although training is required for anyone listed on the TCP, export controls training is available to anyone at the University if they so desire.
TCP Recertification

All TCP’s must be recertified by the Responsible Person on an annual basis. OEC has established a schedule for the review of each TCP, and will contact the Responsible Person to begin the process of recertification. This process insures that TCP for projects that are no longer active are terminated (note: TCP’s can only be terminated if there are no export controlled materials in the possession of the any of the project members.) It also ensures that the project personnel list is up to date, that any new project personnel are listed, screened through Visual Compliance and receive export control training, and that the project is still operating within the original parameters set forth in the original TCP in compliance with export control regulations. The OEC reviewer performing the recertification should ask the follow questions of the Responsible Person:

- Is the project is still active or not?
- Has there been a change in scope or a modification of the research project such that new obligations or responsibilities may be imposed upon performance of the project?
- Has there been a change in the sponsor of the research project or are there any additional sponsors of the research project that should be listed on the TCP?
- Have any project personnel originally listed on the TCP left the project?
- If the project has ended, are there any export controlled items, materials, software or data originally listed on the TCP still in the possession of the Responsible Person, or any others initially listed on the TCP?
- If the project has ended and individuals who were originally on the TCP have left the University and still maintain export controlled technology or data, then an NDA must be sent to that individual documenting their continuing obligation to protect this export controlled technology or data.
- Are there any new project members?
- Are there any additional export controlled items that have been received on Grounds related to this project that have not yet been added to the TCP?
- Has any of the information furnished on the original TCP changed, such as room locations, security measures, or other parameters?

If there are new project personnel, they must be screened through Visual Compliance and have export control training as soon as possible, but definitely before they can be added to the TCP and have access to the controlled item(s). This can be delivered in person by OEC, or via the CITI online export control training, which can be accessed through the OEC website.

All personnel listed on a TCP are required to complete export controls refresher training annually (or sooner should circumstances warrant additional training) after the final approval of the initial TCP by OEC. Documentation of follow-up training should be kept in the TCP file and documented on the TCP
Details of the recertification process should be logged in the OEC tracking log. Any TCP’s that are terminated should be moved from the folder for active projects to the closed projects folder (S/FOC/Export Controls/Forms/Technology Control Plan/TCP-Closed/Responsible Person last name (associated sponsor or project).

Export Authorization (Licensing)

If a project is export controlled and a license is needed to involve a foreign national, the Office of Export Controls or another Empowered Official may apply for an export license to allow the disclosure of information to that foreign national. Each individual foreign national whose participation requires a license must be specifically identified in the license and licenses are situation or case specific; open or generic licenses are not available. It is important to note that a TCP, as described above, must be implemented for all projects when access or participation in the project would require foreign national licensing. The Office of Export Controls, at the request and with the assistance of the principal investigator, will prepare and sign the necessary documentation for obtaining a license. The principal investigator, his department and the School are responsible for all costs associated establishing and maintaining security as required under the TCP and all costs associated with project or program activities.

International Travel Reviews and Travel Related License Exceptions and Exemptions

Purpose: Travel to destinations outside the U.S. with controlled items, including controlled information (e.g. UVA or third party proprietary or confidential, U.S. government restricted), may also implicate export control regulations. A license may be required depending on which items are taken, which countries are visited, the purpose of the trip, the specific individual or entity the traveler will be visiting or whether services are provided to a foreign person. It is important to note that presenting results at a scientific conference OUTSIDE of the U.S. is an export and depending on the material to be presented, openness of the conference, location, and sponsor(s) may in some cases require a license. However, an exception or exemption from license requirements may exist. The OEC can determine whether, for those UVA faculty, staff or students traveling internationally on University business and/or with University-owned property, their travels will invoke U.S. export controls, and whether they may need a license to proceed.

Reviews of international travel on University business

- University travelers traveling on University business or with University-owned property should contact the Office of Export Controls well in advance of any planned international travel. This includes trips on university business, as well as personal trips where University-owned property is taken.
University travelers planning international travel should contact the OEC for three possible reasons, depending on the nature of their travel:

- If the traveler is traveling to a country sanctioned by the US Government, the traveler should complete the Sanctioned Country Review Request form available on the OEC website at http://export.virginia.edu/international-travel.

- The countries which will trigger the requirement to use the form and receive written approval from OEC are the countries subject to comprehensive sanctions (Iran, North Korea, Cuba, Syria, and the Republic of Sudan).

- It is strongly recommended that travelers going to countries subject to limited sanctions also complete the Sanctioned Country Review Request form and receive guidance from OEC prior to travel. These countries currently include Belarus, Burma (Myanmar), Central African Republic, China, Cote d’Ivoire (Ivory Coast), Cyprus, Democratic Republic of the Congo, Eritrea, Haiti, Iraq, Lebanon, Liberia, Libya, Somalia, South Sudan, Sri Lanka, Ukraine (Includes entities in Russia), Yemen, Venezuela and Zimbabwe. As the countries subject to U.S. sanctions and the extent of the country-specific sanctions may change at any time, it is advisable to check with the Department of State for the most recent information. See http://www.pmddtc.state.gov/embargoed_countries/index.html. The Department of the Treasury should also be consulted for its OFAC sanctions and the countries listed may be accessed here https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

- If the traveler is taking University-owned items, including UVA or third-party proprietary, confidential or U.S. government restricted information, UVA-owned intellectual property or UVA-owned equipment, the Temporary Export Request Form must be completed by the traveler and returned to OEC for review. This form may be accessed on the OEC website at http://export.virginia.edu/international-travel.

- If the traveler is traveling on University business but not taking any equipment and is not going to a sanctioned country, while not mandatory, the traveler is advised to contact OEC for guidance regarding the international destination by sending an email to export-controls@virginia.edu. The email should include the following information:
  - Dates of Travel
  - Countries that will be visited
  - The purpose of travel
  - Any conferences or meetings that the traveler will attend
• If any transfers of controlled (e.g. proprietary, confidential or restricted) information will occur
• Any other pertinent information

• Upon OEC’s receipt of notification of planned international travel by faculty, staff, or students on University business, or with University-owned equipment, OEC will initiate a review of the planned trip to ensure that no export control regulations will be violated.

  o Review of trips to sanctioned countries.
  
  ▪ Travel to sanctioned countries will garner a high level of scrutiny from OEC as it is fraught with risk for both the University and the individual traveler.

  • OEC will perform a Visual Compliance screen of any individuals and organizations the traveler will encounter. A list of restricted parties will be generated and given to the traveler to review.

  • OEC will review the country-specific sanctions and determine whether a license for the travel will be required, and if a license is required, whether there may be a license exemption available.

  • Any University equipment being taken will have its Export Control Classification determined (see SOP for classification.) The regulations pertaining to the item will be checked for export control restrictions to the designated countries.

  ▪ If any restrictions to the country are discovered for the classified item, a license exception or exemption (see below) will be sought. If none exists, OEC will advise the traveler of the likelihood of a license being issued for the export. If the traveler wishes, OEC will apply for a license on their behalf.

  • OEC will inquire about any exports of technical information that may occur as a result of speaking engagements, meetings, or attending conferences.

  • All documents submitted as a part of the review, as well as the form (with the OEC section completed), will be filed.

  o Review of exports of University owned equipment hand-carried by University travelers on international trips.

  ▪ A list of restricted parties will be generated for each country the traveler plans to visit and will be provided to the traveler.
Unless the items are clearly innocuous, a classification for the items will be sought.

After classification is completed, an evaluation shall be performed to ascertain the export control status of the item to the traveler’s destination.

If a license is required to the destination, the OEC will attempt to overcome the licensing requirement through the use of license exceptions.

If no exception is available, OEC will advise the traveler of the likelihood of a license being issued for the export. If the traveler wishes, OEC will apply for a license on their behalf.

All documents submitted as a part of the review, as well as the form (with the OEC section completed), will be filed.

- Review of University travel to non-sanctioned countries where the traveler will not be bringing any University equipment.

A list of restricted parties will be generated for each country the traveler plans to visit and will be provided to the traveler.

Any declared interactions with foreign parties and organizations will be investigated for inclusion on restricted party lists via a Visual Compliance screening.

Any declared exports of technical information will be investigated for export control implications.

License Exceptions and Exemptions

A License Exception\(^78\) 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 University 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\(^79\) without first consulting with the Office of Export Controls.

---

\(^78\) EAR § 740.1

\(^79\) This list is current as of the date of this writing, but is subject to change. A current list is available at EAR § 742.1.
A License Exemption\textsuperscript{80} may be available for ITAR controlled technical data transmitted outside the U.S., in certain limited situations, 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 University of Virginia or the U.S. Government and is not an employee of a foreign subsidiary;
3. if the information is classified, it will be sent overseas in accordance with the requirements of the Department of Defense Industrial Security Manual; and,
4. no export will be made to countries listed by ITAR § 126.1 or to persons considered generally ineligible under § 120.1(c).

Please note that other exceptions or exemptions may be available.

Any individual intending to travel or transmit export controlled items, technical data (ITAR) or technology (EAR) outside the U.S. must first consult with the Office of Export Controls. The Office of Export Controls has the final authority on the applicability of the proposed license exception or exemptions and may consult with counsel if necessary in making that determination. All exceptions or exemptions must be documented and the record maintained for at least five years\textsuperscript{81} after the termination of the project or the travel return date.

Training & Information

Purpose: Providing general awareness information and training is the foundation of a successful export compliance program. Well-informed personnel minimize the likelihood that inadvertent violations of the law will occur. The greatest risk of non-compliance with 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.

\begin{itemize}
  \item The Office of Export Controls (OEC) will acquire or prepare updated training materials and will ensure that employees and students engaged in University export controlled projects or activities receive the appropriate instruction. The OEC will also maintain records of training provided.
  \item General export control information will be available for the university community online at the following link: \url{http://www.virginia.edu/sponsoredprograms/exportcontrols/index.html}. This website will also provide access to University export control policy, procedures (including this manual), templates and forms.
  \item Deans, directors, or department heads will assist the OEC in implementing the export control training sessions or briefings relative to their respective schools, departments, centers, or
\end{itemize}

\textsuperscript{80} ITAR § 125.4
\textsuperscript{81} ITAR § 125.6 and EAR § 762
institutes. In addition, the directors of other offices or units on campus including, but not limited to: Office of Sponsored Programs, Procurement and Supplier Diversity Services, Environmental Health and Safety, Human Resources and International Studies Office will assist the OEC in implementing export control training sessions or briefings relative to their units.

General Awareness

- The OEC shall be responsible for increasing general awareness on grounds of export controls. OEC employs the following procedures to increase general awareness of export controls.
  
  o Basic information on export controls and contact information for the Office of Export Controls is provided to new employees via email within their first month of employment.
  
  o An annual reminder email will be distributed to all University employees. These emails provide topical information and include contact information for the Office of Export Controls, including a link to the OEC website where faculty, staff and students may access additional information on export controls.
  
  o The OEC offers generalized and tailored export controls presentations at department meetings, informational sessions open to the entire University, to lab groups and for any other gathering where a brief talk about export controls would be useful to the audience.

Personnel Listed on a TCP

- All personnel listed working under a TCP must complete initial training prior to being authorized for access to items and information subject to the TCP. Annual refresher training is also required for any individuals listed on a TCP.
  
  o Those that are required to undergo export control training may choose from an in-person session delivered by OEC staff, or online training provided through UVA’s subscription with CITI (Collaborative Institutional Training Initiative). CITI training may be accessed by going to the OEC website here: http://export.virginia.edu/training.
  
  o Personalized training for those listed on a TCP that is provided by a member of the OEC is generally more tailored to the specific circumstances for the TCP than through the CITI training. However, the CITI training is comprehensive in scope and recommended for those not wishing to have personalized training from OEC.
**Project or Program Specific**

- The Office of Export Controls will provide Project or Program specific training to address identified needs or upon request. Individuals wishing to request training should contact the Office of Export Controls directly at 434-982-5725 or export-controls@virginia.edu.

**Export Control Certification for I-129 Foreign National Employee Petition**

Changes made by the U.S. Customs and Immigration Service to the I-129 Foreign National Employee Petition/Petition for a Nonimmigrant Worker on 11/23/10, require that UVA review new foreign national employees that are applying for an H-1B, H-1B1, L-1 or O-1A visa to certify that it has reviewed the U.S. export control regulations and has determined that (a) an export license is not required to release technology to the prospective employee; or (b) if an export license is required, it will not release controlled technology to the foreign national employee until it has received a license or other authorization to do so.

The certification now required by USCIS is a mandatory requirement that must be satisfied by the employer before the petitioner or prospective employee may submit the I-129 form to USCIS in support of their visa application. More information may be found on the USCIS website by going here: [http://www.uscis.gov/i-129](http://www.uscis.gov/i-129). Additionally, the UVA Human Resources Compliance and Immigration Services group has information on their website, such as an H-1B visa packet. See [http://www.hr.virginia.edu/other-hr-services/CIS/](http://www.hr.virginia.edu/other-hr-services/CIS/) and [http://www.hr.virginia.edu/other-hr-services/CIS/immigration-services/immigration-packets/](http://www.hr.virginia.edu/other-hr-services/CIS/immigration-services/immigration-packets/).

**Submitting the I-129 Export Certification Request Form**

When a department intends to hire a foreign national employee on any of the above-referenced visas, they should submit an I-129 Export Certification Request form to the OEC for review and action. The form is found on the OEC website here: [http://export.virginia.edu/i-129-export-certification](http://export.virginia.edu/i-129-export-certification).

**Submission Instructions**

- The I-129 Export Certification Request form should be submitted by someone, usually in the hiring department, that has access to the following information:
  
  o Personal information about the foreign national;
  o Knowledge of the foreign nationals job duties and responsibilities; and
  o Knowledge of the funding sources supporting the foreign national’s position and, if applicable, any research program or project the foreign national will be participating in.

- Form should be submitted electronically, by one of the following means:
Form Only – use the submit button on the bottom of the form; or

Form & Supporting Documents – save the completed form as a pdf, and then email it with the supporting documents to export-controls@virginia.edu with “Export Certification Request for I-129” in the subject line of the email.

OEC Review & Documentation Process

- The OEC staff member will create a file on the shared drive in I-129 folder using the following naming convention: Last Name, First Name.

- OEC will review the information provided in the Export Certification Request form.
  - If incomplete, OEC will request more information from the supervisor or submitter.
  - If complete, OEC will print the submitted form to individual’s file using the following naming convention: LastName_FirstName_ExCert_YearMonthDay.pdf.

- OEC will then run a Restricted Party Screening on the foreign national through Visual Compliance and address any resulting red flags or issues of concern.
  - The comment in the Visual Compliance RPS screening comment field should read “I-129 Export Certification”
  - OEC will save the screening results to individual’s file using the following naming convention: LastName_FirstName_RPS_YearMonthDay.pdf.

- OEC will search for the foreign national in the UVA online directory.
  - If found, OEC will save a copy of the directory page to individual’s file using the following naming convention: LastName_FirstName_Directory_YearMonthDay.pdf.
  - If not found, no additional action is needed.

- OEC will complete the Review section of the Request form (Section E, OEC use only).
  - If the foreign national will be funded by a sponsored program, review the funding announcement (BAA, RFP, RFQ, etc.), the terms and conditions of any sponsored awards, and any other referenced documents.
  - Note the presence or absence of the following:
• Specific reference to export controls
• Citizenship restrictions
• Publication restrictions
• Development work
• Proprietary, confidential or restricted information
• Deliverables other than scholarly or scientific presentations and papers
• Other indications that the work either is or is not fundamental research

  o Review any listed technology and technical data:

    ▪ Determine the regulatory jurisdiction.
    ▪ Determine the appropriate ECCN or USML category.
    ▪ Determine if a license is required to export technical data or technology to the foreign national employee.
    ▪ Determine if a license exception or exemption is available to overcome any license requirement.
    ▪ In the space provided in section E, record any sponsored awards, how any restricted party screening results were resolved, and choose the “Recommendation” (e.g. Option #1 – No License Required, etc.)

  o Print the completed form to the individual’s file using the following naming convention: LastName_FirstName_Review_YearMonthDay.pdf.

Advisory Letter

• Select the appropriate OEC Advisory Letter template:

  o “Advisory Letter RESEARCH without EC.doc” – use this template when the employee will be conducting research, but no export license requirements have been identified.

  o “Advisory Letter RESEARCH with EC.doc” – use this template when the employee will be conducting research, and export license requirements have been identified.

  o “Advisory Letter NON RESEARCH.doc” – use this template when the employee is a medical professional who will not be conducting research and no export license requirements are identified.

  o “Advisory Letter NON RESEARCH Non Health” – use this template when the employee is not a medical professional, will not be conducting research, and no export license requirements are identified.
Customize the Advisory Letter template:

- Address the letter to the supervisor or principal investigator (PI)
- Copy the letter to the foreign national if at UVA
- Copy the letter to the submitter if other than the foreign national or supervisor/PI

Response

- All communication should be made via email for documentation purposes.

- The email issuing the Advisory Letter should also include a copy of the completed Export Certification Request form that was originally submitted to OEC (not the version with the OEC comments included).

- The email should be addressed to the foreign national’s supervisor or principal investigator, copying the foreign national and the submitter if other than the supervisor or principal investigator, and should indicate that the email is in response to the Export Certification Request received from the submitter on the date submitted related to the foreign national’s pending visa application. State that the export review is and certification process is necessary to comply with the U.S. Customs and Immigration Services’ requirements for certain visa types. Both the Export Certification Request form and the Advisory Letter should be attached to the email. State in the email that if the information in the attached documents is correct, they should include the Advisory Letter in the visa packet to be submitted to UVA Human Resources. If the information is incorrect, ask that they contact OEC immediately to correct this information or to answer any questions. The email should also remind the supervisor or principal investigator that physical exports of items are subject to export controls regardless of whether or not they were generated in the course of performing fundamental research and such exports may require an export license. Transfers to foreign nationals, wherever located, of technical data identified in the export regulations may also be subject to licensing requirements. State in the email that should they ever need to export items, devices or technical data to foreign collaborators or subcontractors/subawardees, they should contact the OEC for guidance with any necessary licensing requirements.

Timeframe

- The standard office procedure is to issue an Advisory Letter within two business days of submission of the Export Certification Request form, unless red flags are found during the initial screening or insufficient information has been provided to OEC and OEC is waiting for further data.
Recordkeeping

The University’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 University record retention policy, and shall be retained for no less than five years after the project’s TCP termination date, last date of export, license termination date, or other time-point identified in the applicable regulations. Should a discrepancy exist between the University’s retention policy and an applicable export regulation, documents will be retained for the longer period.

A copy of the approved TCP will be maintained by the Office of Export Controls. Documentation associated with OEC reviews, technology assessments, agency submissions (e.g. commodity classification, commodity jurisdiction, export authorization, and advisory opinion requests) and other process will be maintained by the OCE. Records associated with physical exports shall be retained by the University office or unit initiating the shipment (i.e. performing the export).

Under the ITAR, when an exemption is claimed for the export of unclassified technical data, the exporter must maintain a record of each such export. The business record should include the following information: a description of the unclassified technical data, the name of the recipient end-user, the date and time of the export, and the method of transmission. Note that this section of the ITAR does not specify a required retention period.

BIS has identified specific record-keeping requirements in the EAR. 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.

Internal Monitoring

In order to maintain the University’s export compliance program and ensure consistent adherence to U.S. export laws and regulations, the OEC may conduct internal reviews of TCPs and certain projects as deemed appropriate. The purpose of such reviews is to identify (1) possible violations; (2) deficiencies in training, procedures, etc. that can be corrected or improved; and (3) assure that projects remain in compliance when there are changes to the applicable regulations or sponsor terms and conditions.

Violations

It is the policy of the University of Virginia to voluntarily disclose violations as required. Since September 11, 2001, U.S. government agencies have dramatically increased the investigation into and successful prosecution of export control regulation violations. The penalties for these violations can be

82 ITAR § 123.26
83 EAR § 762.6
very severe, may lead to civil or administrative proceedings as well as criminal prosecution. Potential consequences for the University include fines, debarment and imposition of mandated corrective actions. Personal liability may be imposed upon the individual(s) charged with committing the violation and the penalties include monetary fines, imprisonment, or both, depending upon whether the violation was willful, grossly negligent or inadvertent. However, government agencies assign great weight to voluntary self-disclosures of violations as a mitigating factor.

Any individual who suspects a violation has occurred must immediately notify the Office of Export Controls or another Empowered Official, and only an Empowered Official. The OEC will review the allegation or concern in consultation with the Office of General Counsel. If there appears to be merit to the allegation, OEC will send an initial notification about the suspected violation to the appropriate government agency. If the initial review determines that the allegation or concern is not actually related to export control or lacks merit, it will inform the individual and internally transfer the report to the proper office for further review and resolution, as appropriate. The OEC will conduct a thorough internal review of the suspected violation by gathering information about the circumstances, personnel, items, and communications involved. Once the internal review is complete, the OEC will provide the government agency with a supplementary letter which will include 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;
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. UD’s commitment to export controls compliance.

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

In addition and if appropriate, the OEC may task the Export Controls Advisory Committee to review the information gathered by the OEC and provide recommendations for improving University controls to prevent similar violations in the future. These recommendations, if appropriate and completed within the necessary timeframe, will be incorporated into the University’s supplementary letter to the agency.

84 See responsibilities of the responsibilities assigned to University employees, trainees and students in University of Virginia Policy: Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of Research and Scholarship (Policy ID: FIN-043).
85 EAR § 764.5 and ITAR § 127.12(c)
APPENDIX I: UVA POLICY
FIN-043: Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of Research and Scholarship

Date: 11/29/2011 Status: Final [NOTE THIS VERSION IS PENDING FINAL APPROVAL AND HAS NOT YET BEEN PUBLISHED IN THE UVA POLICY DIRECTORY.]
Policy Type: University
Contact Office: Office of Export Controls, Finance Outreach and Compliance (new link: http://export.virginia.edu)
Oversight Executive: Executive Vice President and Chief Operating Officer, Vice Provost for Research
Applies To: Academic Division, Medical Center, and the College at Wise.
Table of Contents:
Policy Statement

1. Activities & Technology Subject to U.S. Export Controls
2. Thesis or Dissertation Submissions
3. Promotion and Tenure Review
4. Sanctioned Countries
5. Responsibilities

Reason for Policy:
The conduct of certain University research, teaching, service and patient care activities may require, generate or otherwise be subject to control under U.S. export control and trade sanction regulations (“Regulations”). Serious penalties, both civil and criminal, can result from violations of these Regulations. This policy serves two purposes in that it provides a formal expression of the University’s commitment to compliance with U.S. export control and sanction requirements, and it describes the general framework that the University has established to support that commitment.
Definition of Terms in Statement:

- **Controlled Activity:**
  An activity involving the export of controlled technology or goods or that due to its nature or the parties involved is otherwise subject to export control, embargo or trade sanction requirements under the jurisdiction of the U.S. Departments of State, Commerce, Treasury, or any other U.S. government agency with export control responsibilities.

- **Controlled Technology:**
  For purposes of this policy, this term includes any item, component, material, software, source code, object code, or other commodity specifically identified on the Commerce Control List [Part 774 of the Export Administration Regulations (EAR)] or U.S. Munitions List [Part 121 of the International Traffic in Arms Regulations (ITAR)]. This term also includes information to the extent required in the applicable Regulation.

- **Export Control Regulations ("Regulations"):**
  For purposes of this policy, this includes the EAR [15 CFR 730-774]; the ITAR [21 CFR 120-130]; trade sanctions administered by the Office of Foreign Assets Control (OFAC) [31 CFR Chapter V, Parts 500-599], U.S. Department of the Treasury; and any other regulations governing exports that are applicable to University activities.

- **Export Controls:**
  Specific government imposed restrictions and limitations on the dissemination of controlled technology, software and other goods (e.g., tissue samples, agricultural products, plants and animals) or services to foreign persons or destinations.

- **Export Denial Lists:**
  These are the lists of individuals and other entities denied U.S. export privileges and include the Denied Parties List, Entity List, Specially Designated Nationals List, Debarred List, and the Unverified List.

- **Foreign Person:**
  A natural person who is not a U.S. citizen, lawful permanent resident (green card holder) or protected individual (formally granted asylum). It also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g. diplomatic missions). An equivalent term used by the Department of Commerce is “foreign national”.

67
• **Technology Control Plan ("TCP"):**
  A document that sets forth the specific physical, electronic and procedural controls that will be taken to prevent unauthorized access to or export of controlled technology. (A template TCP is available on the forms page of the Office of Export Controls website at [http://export.virginia.edu/technology-control-plan](http://export.virginia.edu/technology-control-plan).

**Policy Statement:**
The University discourages any restriction on the ability of its students, faculty and staff to communicate unclassified information to any individuals, including foreign nationals, engaged in research at the University or in the international community of scholars. However, faculty are not prohibited from accepting restrictions so long as those wishing to engage in controlled activities properly assist the University in preventing unauthorized disclosures and exports in compliance with all applicable Regulations. Because export controls place restrictions on the dissemination of non-publicly available technical information, access to certain controlled technology, and provision of services to foreign nationals in the U.S. and abroad, the University has determined that projects proposing to use or produce controlled technology, controlled articles or that involve the provision of regulated services require special review and authorization to ensure that they will not interfere with the University’s core mission.

1. **Activities & Technology Subject to U.S. Export Controls:**
The University shall decide, on a case-by-case basis, whether to sponsor or support a particular export controlled activity proposed by a member of its faculty. Among the factors to be considered in determining whether or not to proceed with a particular activity are its academic merit, compatibility with the core mission of the University, the nature and impact of the restrictions, and the contribution of the activity to the benefit of humanity.

Once the decision has been made to go forward with a controlled activity, the University will only do so once any necessary export license or other authorization from the appropriate regulatory agency has been received. The University shall not engage in business relationships with entities identified on any U.S. government export denial list nor shall it engage in regulated activities with countries or regimes subject to an embargo or sanction program to which the U.S. is a party, without the explicit written authorization of the Office of Export Controls.

Foreign nationals shall be allowed access to controlled technology and may participate in controlled activities to the extent necessary to perform their assigned duties and only to the extent that such access and participation is permitted by the Regulations or authorized in an export license or other instrument issued by the appropriate regulatory agency.
Faculty members wishing to use (or authorize students or staff to use) export controlled technology or work on a project intended to generate export controlled technology, regardless of funding source, must develop a Technology Control Plan (TCP) and have it approved in writing by the Office of Export Controls. (Note: A TCP may not be required if the project only involves EAR-controlled items, does not involve controlled source code or proprietary technical information, and the work will be conducted exclusively in the U.S., but this determination must be made by the Office of Export Controls.) Once the TCP has been approved, it must be attached to the faculty member’s Request to Authorize Research Restrictions and routed to the faculty member’s department chair, dean and the Vice Provost for Research (or designee); each position must support the request for it to move forward in the process. No procurement, grant, contract or other agreement to conduct export controlled activities, or to produce or obtain export controlled technology or software may be finalized until the TCP has been approved and the required University authorizations have been obtained.

2. **Thesis or Dissertation Submissions:**
A thesis or dissertation submitted in fulfillment of a University degree program requirement must not contain information that is subject to export control regulations. Should a student choose to participate in an export controlled activity, any resulting information may be used in a thesis or dissertation only after it has been approved for unlimited public release or dissemination by the appropriate regulatory agency. Students wishing to include export controlled technology in their thesis or dissertation will be required to work with their graduate advisor to develop a TCP or modify an existing approved TCP to detail how all degree requirements will be met while preventing unauthorized exports of controlled technology. This new or revised TCP must be submitted by the student’s graduate advisor to the Office of Export Controls for review and written approval. Following approval of the TCP by the Office of Export Control, the graduate advisor must submit a request that the student be allowed to prepare a thesis or dissertation containing export controlled technology to the department chair and the dean of the student’s degree program and receive their support. The Vice Provost for Research (or designee) must give final approval of any plan to include export controlled technology in a student thesis or dissertation.

3. **Promotion and Tenure Review:**
Decisions regarding the inclusion or exclusion of export controlled activities as part of the promotion and tenure review process shall be determined by the faculty member’s academic department, school, and when applicable, the Provost. However, controlled technology may not be submitted for consideration of promotion and tenure unless and until one of the following has occurred:

a. the information is approved for unlimited public release or dissemination by the appropriate regulatory agency; or
b. the Office of Export Controls has performed an export assessment, provided any necessary training to individuals requiring access to the controlled technology, and documented that one or more of the following permits all proposed exports associated with the promotion and tenure review process:
   i. that an export license is not required;
   ii. a valid license exception exists and any conditions are fulfilled; or
   iii. an export license or other authorization has been obtained by the University and that any attached provisos or conditions can be met.

4. **Sanctioned Countries:**

Certain countries are subject to a comprehensive or near comprehensive program of embargoes and trade sanctions by the US government. The broad scope and applicability of these programs necessitates that the all University activities that are to be conducted in, involve the participation of parties located in, or will benefit a sanctioned country be reviewed and authorized by the Office of Export Controls. The following are examples of activities that are subject to control under these regulations:

- Import of goods originating in a sanctioned country;
- Direct or indirect export of goods, including both controlled technology and items that are not specifically listed on the CCL or USML (e.g. research samples, basic lab and office supplies) to a sanctioned country;
- University travel to a sanctioned country;
- Provision of a service of value (e.g. research, testing and consulting services) to a party in a sanctioned country; and
- Obtaining services from a party located in a sanctioned country.

The countries currently subject to a comprehensive or near comprehensive program of embargoes and trade sanctions include the following: Cuba, Iran, North Korea, Sudan and Syria. A complete and up-to-date listing of all Sanctions Programs administered by the Office of Foreign Assets Control of the Treasury Department may be found here: [https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx](https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx). For embargoes and other controls administered by the Bureau of Industry and Security of the Commerce Department please see 15 CFR Part 746, found here: [http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear](http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear).

5. **Responsibilities:**

The role of the **Office of Export Controls** is to facilitate the University’s research, teaching, service and patient care mission by administering a program to support this policy; to that end, the Office of Export Controls is responsible for:
• Establishing and administering procedures, forms, and processes to facilitate compliance with this policy;
• Developing and delivering outreach and training materials for University faculty, staff, students and trainees to increase export control awareness;
• Performing restricted party screening, as requested, for persons or entities with which the University will be conducting business or collaborating, including sponsors, collaborators, foreign national employees, visiting scientists or scholars, subrecipients, and subcontractors;
• Providing tools to the University community to assist in the identification and management of export control issues;
• Working with faculty members to develop Technology Control Plans, including IT security measures, and granting final written approval for these Plans;
• Performing all requested 1-129 certification reviews for the University within 2 business days of the initial request and providing the requisite certification letters;
• Performing all requested export licensing assessments for international shipments;
• Conducting assessments, as requested, for international travel;
• Managing the University’s export control related registrations and online accounts with regulatory agencies;
• Advising Authorized Institutional Signatories on export control issues related to contracts (FIN-036) and academic program agreements (FIN-035);
• Seeking export authorizations and clarifications on behalf of the institution as necessary and appropriate to support University activities; and
• Performing compliance monitoring and risk assessment activities.

The Director of Finance Outreach and Compliance is responsible for:

• Providing general oversight of the export controls function (Office of Export Controls) and the direct supervision of the Office of Export Controls staff;
• Serving as an Empowered Official of the University, as defined in the International Traffic in Arms Regulations (22 CFR 120.25), with the independent authority granted by the University in all matters governing foreign trade, export administration, export compliance oversight, investigations, and to stop any transaction or to refuse approval for any action that is deemed not to be in full compliance with the Regulations or University policies governing such action or transaction; and
• Signing and submitting export control and compliance related documents, including, but not limited to, license applications, voluntary disclosures, commodity jurisdiction requests, requests for advisory opinions, export certifications and other export related requests for approval to Federal agencies and other parties in behalf of the University.
• Acting as the University’s secondary or additional point of contact for agencies with regulatory or enforcement authority under the Regulations

The Export Compliance Officer is responsible for:

• Serving as the University’s principal point of contact for agencies with regulatory or enforcement authority under the Regulations;
• Establishing, and revising when necessary, the programmatic framework through which the University manages export controlled activities at the
University, including development and dissemination of policies, procedures, educational materials and website content; Serving as an Empowered Official of the University, as that term is defined in the International Traffic in Arms (22 CFR 120.25), with the independent authority granted by the University in all matters governing foreign trade, export administration, export compliance oversight, investigations, and to stop any trade transaction or to refuse approval for any action that is deemed not to be in full compliance with the Regulations or University policies governing such action;

- Signing and submitting export control and compliance related documents, including, but not limited to, license applications, voluntary disclosures, commodity jurisdiction requests, requests for advisory opinions, export certifications and other export related requests for approval to Federal agencies and other parties in behalf of the University;
- Investigating potential export control violations related to the conduct of University activities;
- Providing outreach, assistance, and training to University faculty, staff, students and trainees regarding the laws, regulations, and University procedures associated with export control; and
- Performing periodic risk assessments to evaluate the relative strengths and weaknesses of the University’s export compliance program and providing the assessment results to the Vice President for Finance and to the Executive Vice President and Chief Operating Officer for their review and action, if appropriate.

Authorized Institutional Signatories, as defined in University Policy FIN-036 and Policy FIN-035, are responsible for:

- Identifying and referring agreements that include export control or sanction compliance risks to the Office of Export Controls for review prior to execution or, at minimum, prior to authorizing work to begin at the University under the subject agreement;
- Understanding that by signing an agreement involving foreign national parties, export controlled activities, or the delivery of export controlled technology to foreign nationals or foreign destinations without prior review by the Office of Export Controls, the Authorized Institutional Signatory is asserting that
  - no export control or sanction related issues/risks exist;
  - no party to the agreement is subject to a U.S. government restriction pertaining to export controls or sanctions and which is applicable to the scope of activities covered by the agreement;
  - the University is not agreeing or committing to compliance with or participation in any boycott, embargo or sanction not explicitly supported by the U.S. government (e.g., the Arab League Boycott of Israel, as detailed in the Export Administration Regulations);
- Ensuring compliance obligations are limited to applicable U.S. export control regulations for work conducted within the U.S.: in cases where other legal jurisdictions may be applicable the Authorized Institutional Signatory must explicitly inform the University unit initiating the agreement of the requirement and that it may be required to pay for the cost of retaining outside legal counsel.
or other compliance experts familiar with applicable non-U.S. laws and regulations; and

- Assuring that, by signing any agreements for the procurement of technology, software or equipment, the agreement requires the vendor to provide any export control classification or categorization information related to the purchased items prior to the full execution of the purchase agreement.

**Faculty members** are responsible for:

- Consulting with and providing assistance to the Office of Export Controls to ensure that:
  - controlled technology, regardless of whether it is instructional or research technology, used or produced by them or under their supervision is categorized and safeguarded correctly under U.S. export control regulations;
  - controlled activities are identified, approved, and licensed if necessary; and
  - all exports of controlled technology, both physical and deemed, including those associated with international travel are conducted in compliance with applicable U.S. export control regulations;

- Understanding and complying with the terms and conditions of their funding awards and other agreements (e.g. sponsored research agreements, nondisclosure agreements, materials transfer agreements, license agreements, etc...), with particular emphasis for the purposes of this Policy on, export control provisions, limitations on publication or dissemination of research data and results and limitations on the participation of foreign persons in the research project;

- Assisting the University in preventing unauthorized exports and applying for government licenses where appropriate;

- When applicable, developing a Technology Control Plan, submitting the plan for approval, and following the requirements of the approved plan;

- Seeking advice from the Office of Export Controls when acquiring proprietary (non-public) information or items via a mechanism other than procurement/purchase as necessary; and

- Ensuring that staff, students, trainees and foreign visitors under their supervision are made aware of any applicable requirements (e.g., University, regulatory, or sponsor imposed) and that they receive adequate training in how to conduct their activities in compliance with those requirements.

**All University employees, trainees and students** are responsible for:

- Knowing and complying with any legal, regulatory or University requirements applicable to their University activities;

- Seeking assistance from the Office of Export Controls prior to performing any export of controlled technology, physical items or software (examples include temporary exports associated with international travel, international shipping, and deemed exports); and

- Reporting any suspected non-compliance with U.S. export control regulations or this policy to the Office of Export Controls.
Procedures:
Export control procedures, forms and templates are posted on the Office of Export Controls (new link: http://export.virginia.edu) website under the Procedures tab.

Related Information:
General information about U.S. export control regulations as well as links to regulations and regulatory agencies are available on the Regulations page of the Office of Export Controls website.

Information about export controls training is available on the Office of Export Controls Training page. This includes information related to the mandatory training required for all personnel listed on a Technology Control Plan.

Information on Restricted Party Screening (RPS) can be found on the Office of Export Controls RPS page. This includes access to the export denial or restricted parties lists issued by various U.S. government agencies that must be consulted prior to any export as well as information about the University’s contracted web-based screening service/tool.

Human Resources, Compliance and Immigration Services, Visa Application Materials (H-1B packets contain instructions on how to obtain the required export certification).

Major Category: Finance and Business Operations
Category Cross Reference: Research Administration
Approved by, Date: Executive Vice President and Chief Operating Officer, 11/29/2011

Maintained by: Policy Directory
Last Modified: 05-May-2015 10:43 am
© Copyright 2015 by the Rector and Visitors of the University of Virginia
APPENDIX II: EXPORT REVIEW CHECKLIST
**Export Control Checklist for OSP**

*Please see instructions on pages 3-6 for guidance*

<table>
<thead>
<tr>
<th>Proposal Review</th>
<th>Proposal #:</th>
<th>Reviewer Initials:</th>
<th>Date:</th>
</tr>
</thead>
</table>

This review may be completed prior to proposal submission or award notification; if not completed at that time, it must be completed as part of the **Award Review** below. *Note: Proposal Review is not applicable to non-financial agreements and may be referenced as “not applicable”.*

1. Is this proposal to a foreign sponsor?   
   - Yes   
   - No

2. Does the proposal involve any foreign collaborators or subcontractors?   
   - Yes   
   - No

3. Does the proposal involve any foreign travel or shipping out of the U.S.?   
   - Yes   
   - No

4. Is the Prime Sponsor NASA, DOE, DOD, DHS or an intelligence agency?   
   - Yes   
   - No
   a. If DOD agency, is funding other than 6.1 (Budget Activity Code 1) indicated?   
      - Yes   
      - No

5. Does the funding announcement (BAA, RFP, RFQ, Topic #, etc…) contain references to any of the following:   
   a. U.S. Government classification or clearance requirements?   
      - Yes   
      - No
   b. “Controlled Technical Information” or Covered Defense Information”   
      - Yes   
      - No
   c. Export Control Language?   
      - Yes   
      - No
   d. Limitations on participation or access based on citizenship/nationality?   
      - Yes   
      - No
   e. Notice to sponsor required for any foreign personnel on the project?   
      - Yes   
      - No
   f. Publication or Dissemination restrictions (any language requiring “approval” versus “review”)?   
      - Yes   
      - No
   g. Information/Data Protection Requirements (confidentiality, sensitive information, “For Official Use Only (FOUO), IT security, etc…)?   
      - Yes   
      - No
This review, in addition to the Proposal Review, above, if not previously completed, must be completed by the pre-award reviewer upon or before notice of award for grants or for contracts/subcontracts upon receipt of the proposed grant or contract/subcontract documents. If the answer is “yes” to one or more questions in either section of this document, the file must be routed to the Office of Export Controls (OEC) for review prior to beginning negotiations or at the very least coincident with beginning negotiations. If this is not possible, or required, the file must be routed to OEC prior to sending the award to the Account Create team for regular or at-risk award setup. (NA=Not Applicable)

1. Does the agreement or grant award terms contain references to any of the following:
   a. U.S. Government classification or clearance requirements? Yes No
   b. “Controlled Technical Information” or Covered Defense Information” Yes No
   c. Export Control Language? Yes No
   d. Limitations on participation/access based on citizenship or nationality? Yes No
   e. Notice to sponsor required for any foreign personnel on the project? Yes No
   f. Publication/Dissemination restrictions (language requiring “approval”)? Yes No
   g. Information/Data Protection Requirements (confidentiality, sensitive information, “For Official Use Only (FOUO), IT security, etc…)? Yes No

2. Is the research or other activity in one of the following fields:
   a. Military/Defense Intelligence, Information, Equipment, Technology, Materials or Systems? Yes No
   b. Information Security or Encryption? Yes No
   c. Aviation or Avionics? Yes No
   d. Satellite, Rocket or Missile Technology? Yes No
   e. Biologics, Toxins or Chemicals? Yes No
   f. Nuclear Technology or Materials? Yes No
   g. Radar or Sonar Technology? Yes No
h. Supercomputers?  
   Yes  No

i. Infrared or Night Vision Devices, Cameras or Technology?  
   Yes  No

3. Is the Prime Sponsor NASA, DOE, DOD, DHS or an intelligence agency?  
   Yes  No

4. Were there any “hits” or “red flags” identified by Visual Compliance for any foreign entities, foreign persons working on the project or for any collaborators or subcontractors on the project?  
   NA  Yes  No

5. Is a DD 2345, Military Critical Technology Data Agreement, included or required?  
   Yes  No

OEC Comments and Instructions:
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

OEC Signature:                    Date:
_____________________________________________________________________________________

Results Distributed
To:
_____________________________________________________________________________________

78
Instructions

PROCESS

An Export Control review must be completed by the OSP pre-award reviewer for all of the following:

- New proposals relating to all of the following funded awards...
- New contracts, including research funding agreements, non-disclosure/confidentiality agreements, license agreements, material transfer agreements, DD 2345 – Military Critical Technology Data Agreements, and data use agreements.
- Modifications to the above-listed contracts if those contracts are identified as having export control issues or requirements and the modification:
  - affects the characteristics of the work being performed (does not include an elimination of an activity, a mere reduction in the level of activity or a continuation of the same activity);
  - pertains to intellectual property, confidentiality, publication, participation of foreign nationals or dissemination/reporting restrictions;
  - involves foreign collaborators or subcontractors; or
  - concerns foreign performance sites, foreign travel or shipping to locations outside of the U.S.
- Grants or Cooperative Agreements:
  - from foreign sponsors;
  - with foreign collaborators or subcontractors;
  - with foreign performance sites or foreign travel planned;
  - from DOD, NASA, DOE, DHS or an intelligence agency; or
  - including any export control language, foreign national restrictions or publication restrictions.

PROPOSAL REVIEW

1. Mark “yes” if the sponsor is an individual or other entity located outside the U.S. and/or not organized to conduct business in the U.S. Mark “no” if the sponsor is located in or otherwise authorized to conduct business in the U.S.

2. Mark “yes” if any collaborator or subcontractor on this project is physically located outside the U.S. or if the collaborating or subcontracting organization is not organized to conduct business in the U.S. It is not required that the citizenship or nationality of any individual foreign collaborator or subcontractor be determined until the export control status of the technology to be exchanged or generated is established. Mark “no” if there are not any collaborators or subcontractors physically located outside of the U.S. or if they are all physically in the U.S. they are organized to conduct business in the U.S.

3. Mark “yes” if the project describes or designates funds for any foreign travel or shipping to locations outside of the U.S. in association with this project. Locations in Antarctica,
international waters, and the international space station are considered “foreign” for the purposes of this form.

4. Mark “yes” if the prime sponsor (any sponsor) is any branch, division or agency within NASA, DOD, DOE, DHS, or any intelligence agency.

   a. Mark “no” if the funding announcement (BAA, RFP, etc…) lists the type of funds as Category 6.1 (Basic Research) or Budget Activity Code 1. You should also mark “no” if the funding announcement does not indicate the type of funding. The following is a list of current DOD Budget Activity Codes (BAC) and a brief description:

      i. BAC 1: Basic Research
      ii. BAC 2 (formerly Category 6.2): Applied Research
      iii. BAC 3 (formerly Category 6.3): Advanced Technology Development
      iv. BAC 4 (formerly Category 6.4): Demonstration and Validation
      v. BAC 5 (formerly Category 6.5): Engineering and Manufacturing Development
      vi. BAC 6 (formerly Category 6.6): Management Support
      vii. BAC 7 (formerly Category 6.7): Operational Systems Development

5. Review the funding announcement and mark whether or not any of the following are present:

   a. U.S. Government Classification or Clearance Requirements – all items, information or projects which are subject to U.S. Government classification or clearance (personnel or facility) requirements, are, by definition, export controlled. There are three levels of classification or clearance used by most agencies, which are designated “confidential”, “secret”, and “top secret”. The Department of Energy designates “L” and “Q” levels, which are essentially equivalent to “secret” and “top secret”, respectively. Two additional terms, which indicate a clearance requirement, are “Sensitive Compartmentalized Information” (SCI), and “Special Access Program” (SAP). These designations indicate additional controls beyond those associated with the clearance or classification level.

   b. Export Control Language – any export control language other than a generic statement or clause indicating that all parties must abide by applicable U.S. export control laws and regulations or that export control regulations may apply to this project AND you have marked “no” to all other review criteria.

   c. Limitations on Participation or Access Based Upon Citizenship or Nationality – a requirement that project funds only be expended to support U.S. persons/students (without any further limiting language) is not typically considered a limitation on participation or access for export controls purposes (this type of limitation has been seen in certain USDA or DOT programs).

   d. Sponsor Approval of Personnel Based Upon Citizenship or Nationality – this includes prior notice provisions where the sponsor requests prior notice of any foreign persons on the project.
e. Publication or Dissemination Restrictions – any language that indicates that a sponsor has the right to “approve” any publications before they are published constitutes a publication restriction. Language that indicates that a sponsor may review the proposed publication and request a delay to accommodate deletion of any proprietary information prior to publication, within a reasonable time frame not to exceed 90 days (60 days is preferable), is not considered a publication restriction for export control purposes.

f. Information/Data Protection/IT Security Requirements – examples include, but are not limited to, DFARS 252.204-7012 (“Covered Defense Information”, including “Controlled Technical Information”), “Protected Critical Infrastructure Information, specific NIST 800-83 standards, certain NIST 800-171 standards, a Non-Disclosure/Confidentiality Agreement or clause within a research funding agreement, etc...).

AWARD/AGREEMENT REVIEW

1. Review the Agreement or Award and mark whether or not any of the following are present:

   a. **Classification or Clearance Requirements** - all items, information or projects which are subject to U.S. Government classification or clearance (personnel or facility) requirements, are, by definition, export controlled. There are three levels of classification or clearance used by most agencies, which are designated “confidential”, “secret”, and “top secret”. The Department of Energy designates “L” and “Q” levels, which are essentially equivalent to “secret” and “top secret”, respectively. Two additional terms, which indicate a clearance requirement, are “Sensitive Compartmentalized Information” (SCI), and “Special Access Program” (SAP). These designations indicate additional controls beyond those associated with the clearance or classification level.

   b. **Export Control Language** – any export control language other than a generic statement or clause indicating that all parties must abide by applicable U.S. export control laws and regulations or that export control regulations may apply to this project **AND you have marked no to all other review criteria.**

   Whenever possible, attempt to include language similar to the following: “No disclosure or transfer of information, technology, technical data, software, source code, equipment or materials identified on a U.S. export control list (hereinafter “export control-listed material”), including, but not limited to, the Commerce Control List (15 CFR 774-7xx) and the US Municitions List (22 CFR 121-1xx), is planned under this Agreement. Should the parties later determine that disclosure or transfer of export control-listed material is essential to the successful performance of this Agreement, the parties agree that no such disclosure or transfer shall occur without first obtaining a duly executed written modification to this Agreement.”

   c. **Limitations on Participation or Access Based Upon Citizenship or Nationality** - a requirement that project funds only be expended to support U.S. persons/students
(without any further limiting language) is not typically considered a limitation on participation or access for export controls purposes (this type of limitation has been seen in certain USDA or DOT programs).

d. **Sponsor Approval of Personnel Based Upon Citizenship or Nationality** – If the review is based upon personnel qualifications only and not residency/citizenship/nationality, then OEC review is not required. However, if the sponsor requests residency/citizenship/nationality information then OEC should be consulted.

e. **Publication or Dissemination Restrictions** - any language that indicates that a sponsor has the right to “approve” any publications before they are published constitutes a publication restriction. Language that indicates that a sponsor may review the proposed publication and request a delay to accommodate deletion of any proprietary information prior to publication, within a reasonable time frame not to exceed 90 days (60 days is preferable), is not considered a publication restriction for export control purposes.

f. **Information/Data Protection/IT Security Requirements** – examples include, but are not limited to, DFARS 252.204-7012 (“Covered Defense Information”, including “Controlled Technical Information”), “Protected Critical Infrastructure Information, specific NIST 800-83 standards, certain NIST 800-171 standards, a Non-Disclosure/Confidentiality Agreement or clause within a research funding agreement, etc...).

2. If the agreement or award involves work in any of the following areas or fields and this has not already been reviewed by OEC at the proposal stage prior to submission:

   a. Military/Defense Intelligence, Information, Equipment, Technology, Materials or Systems?
   b. Information Security or Encryption
   c. Aviation or Avionics
   d. Satellite or Missile Technology
   e. Biologics, Toxins or Chemicals
   f. Nuclear Technology or Materials
   g. Radar or Sonar Technology
   h. Supercomputers
   i. Infrared or Night Vision Devices, Cameras or Technology

3. If the Prime Sponsor (whether UVA is the prime recipient/contractor or a subrecipient/subcontractor) is any division of NASA, DOD, DOE, DHS or any intelligence agency, or a foreign entity, then the agreement or award must be reviewed by OEC prior to execution.

4. All foreign entities (for this part of the review, assessment is limited to foreign companies, institution or organizations associated with the agreement or award, not individuals unless they are a named party to the agreement or award such as an independent consultant or independent contractor/subcontractor), including, but not limited to, subcontractors, sponsors, collaborators and vendors, associated with the award must be screened through Visual Compliance prior to execution of the agreement. If there are no foreign entities associated with
this award then the response should be “NA”.
Screening may be conducted by OSP Pre-award reviewers and OEC is available to provide training for Visual Compliance screening. If OSP Pre-award reviewers are not able to perform this screening please notify OEC so that OEC may proceed with the screening. If, after screening, there are no “hits” or “red flags” identified by Visual Compliance this should be noted on the checklist and in the file. What constitutes a “hit” or “red flag” is covered in the Visual Compliance training. All questions regarding potential “hits” or “red flags” should be directed to OEC. OEC will work with the PI and the Pre-award reviewer to resolve all such hits or red flags.

5. Indicate whether or not there is a DD 2345 – Military Critical Technology Data Agreement required for this project.

OEC COMMENTS AND INSTRUCTIONS

This section will be used to provide further instructions to the OSP Pre-award reviewer, to specify which projects, if any should be flagged in Oracle as “export controlled” and to provide any further information pertaining to export control issues. Any questions pertaining to this section or to any other parts of this Checklist should be directed to the Office of Export Controls by email to export-controls@virginia.edu, by calling Kathryn Kim at 434-982-1539 or by calling LaVerne Harris at 434-924-0855.
APPENDIX III: TEMPLATE TECHNOLOGY CONTROL PLAN
Statement of Institutional Commitment

The University of Virginia is committed to complying with applicable export control, embargo and trade sanction laws and regulations in all university activities. This commitment is articulated in University policy FIN-043 Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of Research and Scholarship and the associated Export Control Management Program. This Technology Control Plan (TCP) identifies the specific measures that will be taken by Responsible Person, a UVA executive or faculty member unless prior approval is obtained from the Office of Export Controls (OEC), and all project personnel to ensure compliance with those requirements.

Responsible Person  
Department  

Covered Items and Information

The following items or information have been determined to be subject to export control requirements which require that the University place limitations on who may have access to or use the items or information, hereinafter called Covered Items and Information. A variety of factors must be taken into account to determine who may have access to Covered Items and Information; for this reason, only individuals who are identified below and have been approved by the Office of Export Controls may have access.

A list of the Covered Items and Information that will be protected under this TCP is provided in the table below:

<table>
<thead>
<tr>
<th>#</th>
<th>Name or Description</th>
<th>Type</th>
<th>Jurisdiction</th>
<th>Classification*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
As a result of this determination, the Responsible Person, identified above, has worked with OEC to develop this TCP to ensure that Covered Items and Information are adequately protected from disclosure to foreign persons without an approved license, valid license exception, or other written government approval.

Security Overview

“One Lock” is the principal of securing items and information by using at least one mechanism to prevent access by unauthorized persons. This is the minimum requirement for safeguarding the Covered Items and Information, listed above. Methods for obtaining at least “one lock” are described in the physical and information security sections below. Project personnel are responsible for safeguarding Covered Items and Information at all times by having “one lock”; this includes preventing visual access if such access could provide technical information about an item.

Physical Security

Work Area. Locations where work is to be performed with Covered Items and Information shall have restricted access. Restricted access is defined as having a clearly defined perimeter, which is adequate to protect against oral, in the case of discussions involving Covered Information, and visual disclosure of the Covered Items or Information. Physical barriers are strongly recommended but are not required as long as oral and visual disclosure can be prevented. Project personnel within the Restricted Area shall be responsible for challenging all persons who may lack appropriate access authority.

Specify the location(s) where work will be performed with the covered items and information.

Storage. All export Covered Items and Information (hard copies) will be secured in a locked room, storage device or container when not in the personal possession of approved project personnel. Keys or combinations to storage containers used to secure Covered Items and Information will only be issued to the approved project personnel authorized on this TCP. Electronic devices containing Covered Items and Information must be physically secured or

* Provide the applicable US Munitions List category and subparagraph if subject to the ITAR, the Export Control Classification Number (ECCN) if subject to the EAR, or the paragraph and subparagraph if subject to the DoE nuclear regulations.

Note: If more than eight entries are needed, additional space is provided on the last page of this document.
in the possession of an approved user at all times. Note: Security of electronic files should be addressed in the Information Security section, below, rather than here.

Specify the location(s) where the covered items and information (hard copies) will be stored when not in use.

Marking. Whenever possible Covered Items and Information should be clearly marked with an appropriate warning, for example:

**WARNING** - This contains ITAR controlled technical data. Access or dissemination in violation of the ITAR may result in severe administrative (institutional) and criminal (individual) penalties. Contact the UVA Office of Export Controls (x2-1539 or export-controls@virginia.edu) if you find this item/document unsecured. When physical space is limited, an abbreviated warning may be used, for example: **Export Controlled - ITAR.** Watermarks, headers or footers may be used to mark electronic documents.

Describe the markings or warnings that will be placed on covered items and information or explain why they are not practical or possible.

Information Security

**Computer.** All computers used to access or store Covered Items and Information must run Microsoft Windows XP, Windows 7, Vista, Mac OS X, or Linux with the latest security service pack and patches; similar requirements apply to servers and other devices. Generally speaking only approved project personnel should be designated users of computers and servers used to access or store Covered Items and Information and a valid account and password must be provided to gain access. Only approved project personnel retain this login information and no other login accounts are created. Both failed and successful logins are logged internally. Firewalls are installed on all computers to secure and monitor network access to/from the computer. If the firewall must be disabled to allow proper data collection, wired and wireless internet connections must be disabled. Note: Administrative access by central, school or departmental IT personnel must be limited to US persons (citizens, permanent residents or protected individuals).
Data Storage and Transmission. External portable hard drives or flash drives, rather than shared central servers, are recommended for data storage provided physical storage is employed when they are not in use. Drives and devices used to store Covered Items and Information must be password protected or encrypted. For data storage on drives with network access or backup servers, the Covered Items and Information must be secured by encryption and password protection. Email may not be used for the transfer of Covered Items or Information subject to the ITAR or EAR. A secure file transfer method (SSH/SCP/SFTP/SSL) or mailing a disk or flash drive are preferred methods to transfer Covered Items and Information in electronic format. Note: Emailing Covered Items or Information subject to control regimes other than the EAR and ITAR will be considered on a case-by-case basis, but is not authorized unless specified below; when authorized to use email, the sender's is responsible for ensuring that the recipient is physically present in the US at the time of transfer.

Describe any project specific security methods or procedures that will be employed for data storage and transmission.
Supercomputing and Cloud Computing. Unless specified below no supercomputing or cloud computing facilities or services will be used to store, process or transfer Covered Items or Information.

Describe any intended use of supercomputing or cloud computing facilities or services.

Export Control Risks

Award Terms. When the terms of an award contain explicit export control requirements; foreign national restrictions; or require that the sponsor's approval be obtained prior to publication or dissemination of research results, UVA will typically treat the project as subject to US export controls. In such cases, the research results must be identified as Covered Items and Information, above.

Export Control Risks (cont.)

Nondisclosure/Confidentiality. In most cases, proprietary information provided to UVA under confidentiality conditions will be presumed to be subject to US export controls and may not be shared with foreign nationals without the approval of OEC.

Student Involvement. Student participation on projects that require the sponsor's permission to publish or where results are subject to US export controls must be limited to work which is not required for the completion of their degree or program without the explicit approval of the student's Department Chair, Dean's Office and the Office of the Vice President for Research. Students may have access to background proprietary information only to the extent permitted by the applicable export control regulations.

Project Specific Export Authorizations

Specify any intended exports of Covered Items and Information in the section below. Inclusion in this section does NOT, in and of itself, constitute approval to export; it is rather an indication to OEC that an export license or other authorization may be needed. This prohibition on exports includes, but is not limited to, exports to foreign nationals in the US, as well as the permanent or temporary shipment or transfer of Covered Items and Information out of the US.
Special Notes

Use the space below to provide any project specific notes or clarifications.

List any other project specific requirements or conditions in the space provided.

Project Personnel Requirements

Identification: All project personnel needing access to Covered Items and Information must be identified in Appendix 1: Personnel List and sign an Acknowledgement of Responsibilities. The Responsible Person may request the addition or removal of project personnel at any time by submitting a Revised TCP to the OEC (export-controls@virginia.edu).

Training. All project personnel are required to complete the University's export control training program prior to having access to Covered Items and Information or participating in any export controlled aspect of this project. Annual refresher training is required for all project personnel. As part of training, project personnel are made aware of what constitutes an export, their responsibilities to prevent both active and inadvertent disclosures of Covered Items and Information, and of the criminal and civil penalties (including prison sentences of up to 10 years and fines of up to $1M per violation) for failure to comply with US export control laws.

Screening. The OEC will screen all project personnel against the applicable lists of restricted parties and will determine licensing requirements based on their country (ies) of citizenship, nationality, or permanent residence. The Responsible Person shall not allow project personnel access to Covered Items and Information until the individual has signed Attachment A, completed the required training, and been authorized by the OEC. Foreign nationals will only be authorized by OEC once any license requirements have been fulfilled through documentation of an applicable exemption or license exception, or by receipt of an approved export license.
Recordkeeping

US export control regulations require retention of records associated with all exports, use of license exceptions, and certain other activities. The Responsible Party or Department shall be responsible for keeping records for the required five years from the date of the last related activity or longer if necessary to comply with regulatory requirements or the terms and conditions of the award.

End of Project Requirements

Upon completion of this project all Covered Items and Information must be disposed of in accordance with applicable sponsor terms and US export control requirements. Hard copies will be disposed of by cross-cut shredding, incineration or return to the provider; an export license or other authorization may be required for foreign providers. Electronic files will be destroyed by using current “wiping” software. Contact OEC or your department information technology/security administrator for information on effective solutions for wiping. Hardware and equipment can be disposed of properly by contacting OEC; no Covered Items and Information may be surplussed without prior approval of OEC. This TCP must be maintained as long as Covered Items and Information are retained by UVA.

Associated Agreements

It is important that the OEC be able to link this TCP to any associated sponsored programs and other agreements to assure compliance with their terms and conditions. List all agreements, both funded and unfunded, associated with the acquisition and use of the Covered Items and Information in the table below:

<table>
<thead>
<tr>
<th>#</th>
<th>Title or Description</th>
<th>Sponsor or Other Party</th>
<th>Type of Agreement</th>
<th>IT Security Clause (if any)</th>
<th>UVA Project-Award #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internal Notification & Assessment

Notification. The Responsible Person shall notify OEC (1) prior to adding new personnel; (2) when the scope of the project changes; (3) to request modifications to the approved TCP; and (4) when there is a change in funding, or in the
award terms or conditions. The Department shall notify the OEC if (1) the Responsible Person resigns, retires or otherwise ends their employment at UVA; (2) if there is a change in the Principal Investigator on a sponsored award associated with this TCP; or (3) it becomes aware of any deviations from the requirements of this TCP.

**Re-Certification.** The Responsible Person shall certify annually, or at any time upon the request of OEC, to the following: 1) the accuracy of the TCP or if needed provide any necessary updates; 2) that all activities involving *Covered Items and Information* are being conducted in compliance with the approved TCP; 3) that all personnel have completed any required training; and 4) the current status of the project, i.e. completed or ongoing, which necessitated the development of the TCP. Failure to comply with requests for re-certification in a timely manner will result in revocation of approval and notification of the appropriate Department Chair, Dean, and Office of the VP for Research or Provost, as appropriate. Failure to comply with re-certification requirements or with the terms of the TCP may also result in denial of access to sponsored funds for work involving *Covered Items and Information* and may constitute a violation of US export controls.

**Assessment.** The Responsible Person and Department agree to cooperate fully with any compliance checks initiated by the OEC. Checks may be conducted for cause or as part of a random assessment process.

Submitted By: [__________] Date: [_______]

Signature: [__________]

If submitted via email from the Responsible Person's UVA account a signature is not required

OEC Approval By: [__________] Date: [_______]

Signature: [__________]

OEC Assigned [__________] TCP # [__________]
<table>
<thead>
<tr>
<th>No.</th>
<th>Full Name</th>
<th>US Status</th>
<th>Country(ies) of Citizenship/Residency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Name or Description</td>
<td>Type</td>
<td>Jurisdiction</td>
</tr>
<tr>
<td>----</td>
<td>---------------------</td>
<td>------</td>
<td>--------------</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attachment A:
Acknowledgement of Responsibilities for
TCP No. [blank]

By my signature below I acknowledge the following:

1. I have been provided a copy of the Technology Control Plan (TCP), have read and understand its provisions, and intend to abide by its terms and conditions including, but not limited to, only permitting project personnel who have been authorized by the Office of Export Controls (OEC) to access Covered Items and Information.

2. I have completed or will complete prior to accessing any Covered Items and Information the required export control training program specified by the OEC and agree to complete required refresher training for as long as I have access to Covered Items and Information.

3. I understand that I can be held personally responsible for any unlawful disclosures or exports, including transfers to foreign nationals in the United States, of Covered Items or Information. I further understand that individual per violation fines and penalties of up to $1,000,000 and 20 years imprisonment are possible for violations of US export control laws.

4. I understand that my obligation to protect Covered Items and Information continues beyond the end of my participation on this project and my affiliation with the University of Virginia.

5. I understand that if I have questions or concerns regarding the content and implementation of this TCP or about US export control requirements that I should immediately contact the OEC (x2-1539 or export-controls@virginia.edu) for assistance.

I hereby certify that the personal information provided below is accurate and complete.

Full Name: [blank] UVA Computing ID: [blank]

Signature: [blank] Date: [blank]

Signature may be electronic or manual.  If manually signed.

Return signed form to the Office of Export Controls via email to export-controls@virginia.edu.
APPENDIX IV I-129 EXPORT CERTIFICATION REQUEST FORM
Export Certification Request Form

Foreign National Employee (H-1B, H-1B1, Chile/Singapore, and 0-1A) Petitions

_Instructions:_ On 11/23/10 the USCIS released a revised I-129 application form that includes the requirement for an export certification for each foreign national employee. This form is intended to provide the Office of Export Controls (OEC) with information necessary to start the export assessment processes. It is anticipated that an export license will not be required in most cases and that need for export licenses will typically be associated with sponsored research. Should additional information be needed to complete the assessment, the OEC will work directly with the Sponsor/Supervisor identified below. Once OEC has completed the export assessment an advisory letter will be provided to the Sponsoring Department for inclusion in the visa application packet to be submitted to Human Resources.

**Section A: Employee Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>Middle Name</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
</tr>
<tr>
<td>Country of Birth</td>
<td></td>
</tr>
<tr>
<td>Reason for Application</td>
<td></td>
</tr>
<tr>
<td>Country of Citizenship/Residency</td>
<td></td>
</tr>
<tr>
<td>Other Citizenship/Residency</td>
<td></td>
</tr>
<tr>
<td>Current Physical Address</td>
<td></td>
</tr>
<tr>
<td>Permanent Address</td>
<td></td>
</tr>
<tr>
<td>E-mail Address</td>
<td>Provide the UVA e-mail for a current employee; any active e-mail address is acceptable if the UVA e-mail has not been assigned.</td>
</tr>
</tbody>
</table>

**Section B: Position Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title (employee's)</td>
<td></td>
</tr>
<tr>
<td>Sponsoring Department</td>
<td></td>
</tr>
<tr>
<td>Supervisor Name</td>
<td>This should be the Faculty Supervisor or Principal Investigator for Research Scholars or Post-Doctoral Fellows. For faculty or staff positions this should be the employee's direct supervisor.</td>
</tr>
<tr>
<td>Supervisor E-mail Address</td>
<td></td>
</tr>
</tbody>
</table>

List the sources of funding that will be used to support the employee's salary and, if applicable, their research. **Include the UVA award and project number for current funding or, if not yet set-up, the UVA proposal number assigned by OSP.**
Section C: Research Information

Is research is part of the employee’s job description? If yes, provide a brief description of the research project or program in the space below. If a specific project or program has not been determined, describe the specific areas of interest and inquiry that the employee is expected to pursue.

Will the employee be involved in any research or other scholarly activity that is NOT intended for public dissemination? If yes, summarize the export controls, contract terms, publication restrictions, citizenship restrictions, etc. associated with the project below.

Section D: Certification

Name of Person Completing This Form

Phone No.  E-mail  Date
**Section E: OEC Use ONLY**

**Reviewer**  
**Start Date**  
**End Date**  
**Review Type**

**Additional Materials Reviewed:**

**Review Notes:**

**Recommendation**