West Texas A&M University

Export Control

Program Manual

Sponsored Research Services
10/1/2018 updated

List of Common Acronyms

BIS	Bureau of Industry and Security, U.S. Department of Commerce
CCL	Commerce Control List
CJ	Commodity Jurisdiction
DDTC	Directorate of Defense Trade Controls, U.S. Department of State
DFAR	Defense Federal Acquisition Regulation
EAR	Export Administration Regulations
FACR	Foreign Assets Controls Regulations
FAR	Federal Acquisition Regulation
FRE	Fundamental Research Exclusion
ECCN	Export Control Classification Number
ITAR	International Traffic in Arms Regulations
MTA	Material Transfer Agreement
NDA	Non-Disclosure Agreement
OFAC	Office of Foreign Assets Controls, U.S. Department of Treasury
OTC	Office of Technology Commercialization, The Texas A&M University System
PI	Principal Investigator
RPS	Restricted Party Screening
TCP	Technology Control Plan
USML	United States Munitions List

1. Purpose and Background

(a) WTAMU has an obligation to implement an export control compliance program to reduce the risk of export control violations. All employees and students are responsible for the export control implications of their work and must ensure that their activities conform to export control laws and regulations. There are severe institutional and individual sanctions for violations of export control laws and regulations, including the loss of research funding, the loss of export privileges, and criminal and civil penalties.

(b) The export of certain items, technologies, software, and services is regulated for reasons of national security, foreign policy, prevention of the spread of weapons of mass destruction, and competitive trade. Export control laws restrict the shipment, transmission or transfer of certain items, software, technology and services from the United States to foreign countries. Export control laws also restrict the shipment, transmission, or transfer of "deemed exports" which are releases of controlled physical items or controlled information to foreign nationals located in the United States.

(c) Among other regulations, the *Department of Commerce* regulates exports through the EAR 15 CFR 700-799. The *Department of State* regulates exports through the ITAR 22 CFR 120-130, and the *Treasury Department* regulates exports and transactions involving certain countries, individuals and organizations through the OFAC. Each agency possesses different and changing rules and lists for specifying who or what is considered export sensitive and where export controls apply. The restrictions enforced by the OFAC are not affected by ITAR, EAR or the fundamental research exemption established by National Security Decision Directive 189 (NSDD189).

(d) These export control compliance operating procedures are designed to assist WTAMU faculty, staff and students with export control compliance. To the extent these procedures may conflict with WTAMU Rule 15.02.99.W1 *Export Controls*, the Rule takes precedence. Questions on export control procedures may be sent to srs@wtamu.edu.

2. Key Players Responsible for Export Control Compliance

(a) Empowered Official

For all purposes relating to applicable federal export control laws and regulations, the Executive Director of Sponsored Research Services is WTAMU's "Empowered Official". The Export Control Officer and other export area coordinators are responsible for carrying out WTAMU's day to day export control administration. The Empowered Official, assisted by the Export Control Officer, is responsible for authorizing license applications and other approvals required for compliance with export control laws and regulations, and serves as WTAMU's representative and point of contact with federal agencies having export control jurisdiction. The Empowered Official is also WTAMU's official authorized to bind WTAMU in any proceedings with government agencies regarding export control responsibilities and has final responsibility for compliance with export control laws.

(b) Sponsored Research Services

The Sponsored Research Services (SRS) office and other appropriate offices, are responsible for monitoring the export control program and implementing procedures and/or guidelines to comply with federal export control laws and regulations, including developing, implementing and updating these operating procedures.

When requested, the Export Control Officer in SRS will assist other offices and employees in export control assessments to determine, compliance obligations with respect to University activities involving Foreign Persons or international activities under applicable export control laws and regulations, and to determine the applicability of the Fundamental Research Exclusion (FRE)[1] or other exclusions provided by law. The Export Control Officer will also assist with and conduct Restricted Party Screening (RPS)[2] and consult with the Texas A&M University System (TAMUS) Office of General Counsel (OGC) on export control matters as appropriate.

The Export Control Officer and the Empowered Official will conduct periodic assessments of the University's compliance with export control laws and regulations and report the findings to the Vice President of Research and Compliance.

The Export Control Officer is also responsible for developing and implementing procedures to screen proposals and projects for compliance with export control laws and regulations. The Export Control Officer works with the Principal Investigator (PI) to identify and resolve export control issues in the following areas:

1) Reviewing the terms of proposals and agreements to determine whether the research or related activity is export-controlled;
2) Identify factors that can negate the FRE and, if possible, negotiate the deletion of such restrictions;
3) Coordinate with PIs on export-controlled research to ensure the Controlled Physical Items and Controlled Information are secured, that licenses and other authorizations are obtained, and that research is conducted in accordance with the Technology Control Plan (TCP) and;
4) In coordination with any other appropriate offices, ensure that all export control determinations related to a research project are communicated in writing to the PI;

(c) University Administrators

All University employees with managerial or supervisory authority over Foreign Persons or projects involving Controlled Information or Controlled Physical Items should view export control compliance as an important part of their day-to-day responsibilities and are responsible for overseeing export control compliance in their areas of administrative

[1] As defined in TAMUS Policy 15.02, Export Controls and National Security Decision Directive 189, the Exclusion applies to "basic and applied research in science and/or engineering at an institution of higher education in the U.S. where the resulting information either is ordinarily published and shared broadly in the scientific community, or has been or is about to be published."

[2] As defined in WTAMU Rule 15.02.99.W1, Export Controls, determines whether a person or entity is included on the Specifically Designated Nationals and Blocked Persons List or any other list included in the screening software available to the WTAMU community.

responsibility and for supporting the implementation of procedures set forth in this document and as otherwise deemed necessary by the Empowered Official for export control compliance.

(d) Individual Responsibility

All University employees and students, visiting scientists, and other persons retained by or working at or for the University must conduct their affairs in accordance with U.S. export control laws and regulations. While compliance with all applicable legal requirements is imperative, it is equally important to maintain an open research environment that welcomes the participation of researchers from around the world as part of the University mission. To maintain this balance, University personnel must be familiar with the United States export control laws and regulations, including important exclusions and exemptions, as they relate to their responsibilities. Depending upon the nature of their activities and/or job functions, University personnel may be required to participate in formal training as determined by the University's Empowered Official and/or the employees' supervisor.

PIs and other relevant University units are responsible for full compliance with all federal and University export control requirements in the conduct of their research. Violation of the export control laws can directly affect PIs through potential fines, loss of research funding, and/or personal criminal liability. To meet his/her obligations, each PI must:

1) Understand his or her export control obligations and participate in required trainings to be able to identify export control issues;
2) Be aware of the export control indicators below and note such information on any internal compliance or assurance forms;
3) Prior to initiation of research, determine whether any information or technology involved in the research is subject to export control laws or regulations;
4) Periodically review the research to ensure continuing compliance with export control laws and regulations;
5) If undertaking an export-controlled project, work closely with the Export Control Officer to brief the students and other researchers involved in the project of their export control obligations; and
6) Understand that any informal agreements or understandings entered into with a sponsor may negate the FRE or other key exclusions and impose export control obligations on themselves.

3. Identification of Export Control Concerns

3.1 Export Control Red Flags

The following are indicators that an export control review should be conducted to ensure that no violations will occur:

(a) The results of research conducted at WTAMU or by WTAMU employees are intended for military purposes or for other restricted end uses under EAR 99 http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl
(b) Foreign Persons will have access to Controlled Physical Items on campus.

(c) Software including encryption features will be developed or purchased.
(d) WTAMU faculty or staff will export or travel abroad with research equipment, chemicals, biological materials, encrypted software, or Controlled Physical Items; or travel abroad with laptops, cell phones, or PDAs containing Controlled Information.
(e) A proposed financial transaction will involve embargoed countries or entities, individuals located in embargoed countries, or who are on prohibited or restricted end-user lists, as determined by a RPS.
(f) The sponsor requires pre-approval rights over publications or the participation of Foreign Persons.
(g) The project requires the shipping of equipment to a foreign country.
(h) Other Red Flag Indicators: The Department of Commerce, Bureau of Industry and Security has posted a list of Red Flag Indicators for Things to Look for in Export Control Transactions (see http://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators)

3.2 Research

Most data and information involved in University research is excluded from export control regulation under the ITAR or EAR based on several key provisions: (a) the Public Domain Exclusion; (b) the Fundamental Research Exclusion; and (c) the Exclusion of Educational Information. ***Appendix A*** provides additional information on the above exclusions. The benefits of these exclusions can be lost if certain provisions are present in research-related agreements. For this reason, PIs should avoid entering into informal understandings or "side agreements" with research sponsors that restrict Foreign Person access to the research or that impose sponsor controls on the publication or other dissemination of research results. See ***Appendix B*** for a more detailed explanation of the research-related provisions found in agreements.

3.3 Restricted Party Screening (RPS)

To ensure WTAMU is not doing business with individuals or entities that have been debarred, denied export privileges, or are otherwise on one of the numerous government Restricted Party Lists, WTAMU must screen individuals and entities as provided in these procedures. WTAMU has licensed export control compliance software that allows users to screen Restricted Party Lists electronically. To become a user of the software complete the appropriate form at ***Appendix C*** and submit it to the Export Control Officer in SRS. All users are limited to U.S. citizens and legal permanent residents who are full-time employees of WTAMU. If a match is found contact the Export Control Officer in SRS for a secondary screening.

(a) Responsibility to Request Authorization to Visit

It is the responsibility of all faculty, researchers and administrators intending to invite or host International Visitors as indicated in WTAMU Rule 15.02.99.W1, Export Controls, Section 1.3.2, to notify and request approval of such visit from of such visit from their export area coordinator, **before** the arrival of the International Visitor. If you are not a user of the Restricted Party Screening (RPS) software, complete the International Visitors Screening Form found at ***Appendix C*** for the screening. If the RPS results are

of concern and/or impose restrictions, the Export Control Officer will notify the hosting department. If RPS results do not raise concerns the Export Control Officer will notify the hosting department that the visit is approved unless further inquiries are warranted based on additional information that becomes available. A copy of the approval will be provided to the hosting department and will also be retained by the Export Control Officer in SRS.

(b) No Authorization to Access Controlled Information or Controlled Physical Items

No International Visitor may have access (whether verbal, written, electronic, and/or visual) to Controlled Information or Controlled Physical Items unless an export control license has been obtained. It is the responsibility of the faculty, researcher or administrator hosting the visitor to ensure compliance with export control restrictions and to promptly disclose and report to the Export Control Officer or the Empowered Official any violations thereof.

(c) RPS of International Visitors and their Employer

Screening of International Visitors includes the screening of the foreign entity or institution where the International Visitor is employed. Screening is needed whenever a written or verbal invitation to visit WTAMU facilities is made to an International Visitor regardless of whether:

1) The International Visitor is present or not in the U.S..
2) WTAMU needs to sponsor the International Visitor for immigration purposes under the J-1 Exchange Visitor Program.[3]
3) WTAMU does not need to sponsor the International Visitor for immigration purposes because he or she is traveling or has entered the U.S. under the Visa Waiver Program a B-1/B-2 visa or other nonimmigrant visa status as indicated on a properly annotated I-94.

3.4 Technology Screening

In order to ensure that WTAMU is in compliance with all export regulations technology that will be exported must be screened with the same software used for Restricted Party Screening. The software allows for a search of the technology the university plans to export via the Export Administration Regulations (EAR) Commerce Control List (CCL) list and the International Traffic in Arms Regulations (ITAR) / U.S. Munitions List (USML). Contact the Export Control Officer in SRS for a secondary screening if a cross-match is identified.

[3] For example, Foreign Persons may come to visit WTAMU under the J-1 Exchange Visitor Program in the following instances: (a) Sabbaticals with their own funding; (b) Conducting collaborative research funded by their home institution or government; (c) Fulbright or other similar type of sponsorship; and (d) Student internship, paid or unpaid.

3.5 Employment of Nonimmigrant Foreign Nationals

It is important for hiring departments to be aware that the ability to hire nonimmigrant Foreign Nationals for certain positions may be restricted or prohibited by export control laws. For example, nonimmigrant Foreign Nationals may be restricted or prohibited from performing employment responsibilities relating to certain information technology systems positions to the extent the work will involve access to Controlled Information or Items. Supervisors proposing to hire nonimmigrant Foreign Nationals should carefully consider whether or not the proposed employment will involve access to Controlled Information or Items before extending offers of employment. Any export control issues related to the hiring of nonimmigrant Foreign Nationals should be referred to Human Resources who will coordinate with the Export Control Officer as needed.

3.6 International Activities

When WTAMU activities are conducted outside of the U.S., the WTAMU activity organizer and/or responsible international activity official is responsible for seeking and obtaining appropriate export control approvals from the Export Control Officer , for the following activities without limitation: execution of agreements to be performed outside the U.S.; non-credit bearing study abroad courses; and making payments to Foreign Persons. The Export Control Officer or other office(s) with an export area coordinator, in coordination with the Empowered Official, are responsible for developing and implementing procedures to screen international programs and activities for compliance with export control laws and regulations.

3.7 Students Studying Abroad

The Study Abroad Office is responsible for performing RPS on all students enrolled in WTAMU credit bearing programs outside the U.S. RPS is required when the student:

(a) Is a Foreign Person;
(b) Has not previously attended WTAMU; and
(c) Is not enrolled as a continuing student at a college or university based in the U.S..

3.8 Distance Education

Those responsible for offering distance education courses, in cooperation with the Vice President for Academic Affairs, will screen courses as appropriate for purposes of compliance with export control laws and regulations.

3.9 Faculty and Scholars

All Foreign Nationals teaching, conducting research, or presenting workshops, symposia, or other academic presentations who are not employed by WTAMU and are not currently employed by a college or university based in the U.S., should undergo RPS prior to participation in academic or research programs. The inviting department will submit the faculty or scholar information on the RPS form to the Export Control Officer for screening unless they have access to the screening software to conduct the RPS themselves.

3.10 Technology Commercialization

WTAMU does not have a local Office of Technology Commercialization therefore; faculty, staff and students of WTAMU are referred to the TAMU Office of Technology Commercialization (OTC). OTC is responsible for developing, implementing and maintaining procedures to address the export control implications of their work, including procedures related to RPS, invention disclosure screening, etc..

Invention disclosure forms that are submitted to the OTC should be marked by the inventor as export-controlled or not export-controlled. If assistance is needed with the determination contact the Export Control Officer. Per OTC procedures, all disclosures are reviewed by the member Export Control Officer OTC for export control red flags. OTC will conduct RPS on parties with whom it contracts. Any potential export-controlled issues with WTAMU inventions or disclosures will be referred to WTAMU's Empowered Official for recommended handling.

4. Purchasing and Financial Transactions

(a) Vendors

It is the responsibility of the Purchasing Office, in conjunction with the Vice President for Business and Finance, to develop and implement procedures to screen vendors as appropriate for compliance with export control laws and regulations. It is the responsibility of the Purchasing Office to conduct RPS screening of vendors as described in 3.3 *Restricted Party Screening*. Refer potential export control issues to the Export Control Officer. Reference *Appendix E* for the Purchasing Office screening flow chart.

(b) Travel

WTAMU employees and students traveling on WTAMU business or traveling with WTAMU property are responsible for following WTAMU travel policy and complying with export control laws and regulations when traveling outside the U.S.. All foreign travel must be preapproved per *System Regulation 21.01.03, Disbursement of Funds* and the WTAMU Travel Policy.

When planning a trip abroad, travelers should review export control regulations and embargoes. As part of the export control assessment travelers should think about the purpose of their trip, with whom they plan to interact, what they will take, where will they go and how long will they be gone. Items that are not needed should not be taken abroad. Individuals traveling outside the U.S. should consult with the Export Control Officer if they are thinking about taking encrypted software, Controlled Items/Information or unpublished research data or data not in the public domain, or if traveling to an embargoed country to conduct WTAMU activities. Some travel related activities/destinations may be prohibited and other may require a license. The Export Control Officer is available to assist with these assessments and ensure compliance with export control requirements.

Most travel for conferences will fall under an exclusion to the export control regulations (the Publicly Available/Public Domain Exclusion, 22 CFR 120.11 and 15 CFR 734.3). Information that is published and is generally accessible to the public through publication in books or periodicals available in a public library or in bookstores or information that is presented at a conference, meeting, seminar, trade show, or other open gathering is considered to be in the public domain. An open gathering is one in which members of the general public are eligible to attend, and attendees are permitted to take notes.

Although there are a number of exceptions and exclusions which may apply depending upon the facts and circumstances, be aware that traveling outside of the U.S. with laptops, PDAs, cell phones and other data storage devices and encrypted software may require a government license. If employees will need to take a computer with them when traveling outside of the U.S., IT may have a clean computer available to sign out for the trip.

Temporary exports under the "Tools of Trade" license exception apply when the laptop, PDA, cell phone, data storage devices, and encrypted software are:

1) Hand-carried with the individual while traveling,
2) Carried in the luggage or baggage that travels with the individual, or
3) Shipped no more than thirty (30) days prior to the individual's departure or may be shipped to the individual at any time while the individual is outside the country.

Generally, so long as an individual (1) retains his or her laptop computer, PDA, cell phone, data storage devices and encrypted software under their personal custody and effective control for the duration of travel; (2) does not intend to keep these items outside the U.S. for longer than 1 year; and (3) the individual is not traveling to an embargoed country, [4] no government export license is required. Note that this license exception is not available for equipment, components, or software designed for use in/by/with most satellites or spacecraft. "Effective control" means retaining physical possession of an item or maintaining it in a secure environment.

Researchers frequently need to take other WTAMU equipment temporarily outside of the U.S. for use in University research. Often, but not always, the tools of trade license exception applies. Some equipment (e.g., global positioning systems (GPS), thermal imaging cameras, inertial measurement units, and specialty software) is highly restricted and may require an export license, even if one hand carries it. It is important to note that activities involving teaching or training Foreign Persons on how to use equipment may require a license.

A list of some of the travel exemptions and exceptions are more fully described in *Appendix A*. For assistance please contact the Export Control Officer. Reference *Appendix F* for WTAMU's international travel screening form.

[4] See OFAC's Sanctions Program and Country Summaries at http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx for the most current list of embargoed countries and U.S. sanctions.

(c) Shipping

WTAMU personnel or students who are shipping items outside of the U.S. (including hand-carrying items such as research equipment, materials, data, biological materials) are responsible for complying with export control laws and regulations. The simple act of sending a package to a foreign collaborator can result in a violation of export controls. Also shipping to countries subject to embargoes[5] must be cleared by WTAMU's shipping export coordinator in the Purchasing Office.

Mislabeling the package or misrepresenting the classification of the item is illegal. Violations may result in civil penalties on each violation and deliberate violations may result in criminal prosecution with penalties and imprisonment. Under-invoicing or undervaluing an exported item is also against the law.

Shipping regulated items out of the U.S. without a license can result in significant individual fines and imprisonment. This applies to the individual, although there may be fines for WTAMU as well.

The completed and signed WTAMU international shipment export control form (see *Appendix E*) must accompany all international shipment paperwork. Contents of the package are needed for completion of the form. For assistance or questions with international shipments contact the shipping export coordinator in the Purchasing Office.

5. Recordkeeping

Records required to be maintained by export control laws and regulations will be kept for the longer of:

(a) The record retention period required by the applicable export control regulations (see 15 CFR, Part 762 (EAR); 22 CFR, Sections 122.5, 123.22 and 123.26 (ITAR); and 31 CFR 501.601 (OFAC)), or
(b) The period required for the retention of records as set forth in the Texas A&M University System policies and regulations and WTAMU rules.

Records are to be maintained by the office that performs the review operation or as otherwise designated in these procedures.

Maintain export-related records on a project basis. Unless otherwise provided for, all records indicated herein will be maintained consistent with the WTAMU record retention policy, and must be retained no less than seven (7) years after the project's termination date (subject to any longer record retention period required under the applicable export control regulations).

6. Training

[5] OFAC's Sanctions Program and Country Summaries at http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx has the most current list of embargoed countries and U.S. sanctions.

All University employees, including all student employees, are required to take the basic export control Train Traq training course at least once every two (2) years.

Depending on the nature of an individual's activities and/or job functions a WTAMU employee may be required to take supplemental export control training as deemed appropriate by the individual's supervisor and/or the Empowered Official.

7. Monitoring and Auditing

As part of its overall responsibility for directing and monitoring WTAMU's export control compliance program, the Export Control Officer will conduct periodic self-assessments of WTAMU's compliance with export control laws, regulations, and procedures. Processes are continually assessed and updated through discussions within the Export Control Committee to ensure that any deficiencies identified are rectified and appropriate corrective action is implemented. Any deficiencies and recommended solutions are discussed with the Empowered Official and the Vice President of Research and Compliance as appropriate.

The self-assessments review the adequacy of procedures designed to ensure compliance with export control laws and regulations; evaluate controls implemented to ensure compliance with WTAMU's rules and procedures; and test the effectiveness of the controls contained within the Export Control Program.

8. Possible Violations

Each WTAMU employee has the responsibility to report possible violations of U.S. export control laws or regulations. Suspected violations and the details of the suspected violation should be reported to the Export Control Officer or the Empowered Official. Suspected violations may also be reported via the Ethics and Compliance hotline at Ethics Point. Possible violations of U.S. export control laws or regulations will be investigated by the Empowered Official with assistance from the Export Control Officer. The Empowered Official is authorized to suspend or terminate a research, teaching, testing, or other activity if the Empowered Official determines that the activity is not in compliance or will lead to noncompliance with export control laws and regulations. The Empowered Official may determine whether notification to an appropriate government agency is required.

9. Disciplinary Actions

There are severe institutional and individual sanctions for violations of export control laws, including the loss of research funding, loss of export privileges, as well as civil and criminal penalties including imprisonment. Additionally, employees and students may be subject to disciplinary action per TAMUS Policies and Regulations.

Appendix A - Applicable U.S. Laws and Regulations

The following is a summary of selected provisions of the EAR, ITAR, and OFAC regulations. It is intended only as a general guide to understanding and should not be relied upon exclusively. This Appendix should not be used as a substitute for consulting the current version of these regulations, which are subject to amendment from time to time. Any questions should be directed to the Export Control Officer or the Empowered Official.

Three principal U.S. regulatory regimes govern the export of items and technology:

1. *The International Traffic in Arms Regulations (ITAR)*, 22 C.F.R. Parts 120-130, govern the export of defense articles and related technical data (i.e., items or technology that are "inherently military" in nature as well as most space-related items). These regulations are administered by the U.S. Department of State, Directorate of Defense Trade Controls (DDTC). A copy of the consolidated regulations is available at:
http://www.pmddtc.state.gov/regulations_laws/itar.html

2. *The Export Administration Regulations (EAR),* 22 C.F.R. Parts 730-774, govern the export of items or technologies that are commercial or "dual-use" in nature, identified on the EAR's Commerce Control List (CCL). In addition to the regulation of items listed on the CCL, EAR 99 regulates unlisted items and technologies, based on restricted end-uses and end-users. The Anti-Boycott provisions of the EAR prohibit participation in international boycotts that have not been sanctioned by the U.S. government (e.g., the Arab League countries' boycott of Israel). See EAR Part 760 (15 C.F.R. Pt. 760). These regulations are administered by the U.S. Department of Commerce, Bureau of Industry and Security (BIS). A copy of the updated set of regulations is available at:
http://www.access.gpo.gov/nara/cfr/waisidx_99/15cfrv2_99.html

3. For certain prohibited persons or destinations (e.g., Iran, Syria), the export of all items or technologies is generally prohibited under regulations administered by the *Department of Treasury, Office of Foreign Assets Control (OFAC)*. This office administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. The Anti-Boycott provisions of the OFAC prohibit participation in international boycotts that have not been sanctioned by the U.S. Government (e.g., the Arab League countries' boycott of Israel). With the exception of the sanctions against Cuba and North Korea, OFAC sanctions are promulgated under the International Emergency Economic Powers Act of 1977, 50 U.S.C. §§ 1701-1706 (IEEPA). The embargoes against Cuba and North Korea are promulgated under the Trading with the Enemy Act of 1017, 12 U.S.C. § 95a (TWEA).

4. Various other U.S. Government agencies administer limited controls on the export of certain types of items and technologies with which the University may be involved, such as the following: Nuclear Regulatory Commission (nuclear equipment and materials); Department of Energy (nuclear technology, high-energy lasers, etc.); Food and Drug Administration (pharmaceutical development, medical devices); Anti-Boycott Act; Economic Espionage Act; and Anti-Bribery

statutes. Regardless of proper registration with other federal regulatory agencies, export control issues may exist.

ITAR - EXPORT OF DEFENSE ARTICLES AND SERVICES

The International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-130, are promulgated pursuant to Section 38 of the Arms Export Control Act, 22 U.S.C. §§ 2778 *et seq*.) DDTC administers the export and re-export of controlled articles, services, and data from the United States to any foreign destination or to any foreign person, whether located in the United States or abroad. ITAR contains the United States Munitions List (USML) and includes the commodities and related technical data and defense services controlled for export purposes. The ITAR controls not only end items, such as radar and communications systems, military encryption and associated equipment, but also the parts and components that are incorporated into the end item. Certain non-military items, such as commercial satellites and certain chemical precursors, toxins, and biological agents, are also controlled.

ITEMS CONTROLLED UNDER THE ITAR

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

1. Defense Article

Means any item or technical data that is specifically designed, developed, configured, adapted, or modified for a military, missile, satellite, or other controlled use listed on the USML. (22 C.F.R. § 120.6) Defense article also includes models, mock-ups, or other items that reveal technical data relating to items designated in the USML.

2. Technical Data

Means any information for the design, development, assembly, production, operation, repair, testing, maintenance, or modification of a defense article. Technical data may include drawings or assembly instructions, operations and maintenance manuals, and email or telephone exchanges where such information is discussed. However, technical data does not include general scientific, mathematical, or engineering principles commonly taught in schools, information present in the public domain, general system descriptions, or basic marketing information on function or purpose. (22 C.F.R. § 120.10)

3. Defense Service

Means providing assistance, including training, to a Foreign Person in the United States or abroad in the design, manufacture, repair, or operation of a defense article, as well as providing technical data to Foreign Persons. Defense services also include informal collaboration, conversations, or interchanges concerning technical data. (22 C.F.R. § 120.9)

THE USML CATEGORIES

The USML designates particular categories and types of equipment as defense articles and associated technical data and defense services. (22 C.F.R. § 121.1) The USML divides defense items into 21 categories, listed below. An electronic version of the USML is available on the Department of State website at: http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf.

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

CLASSIFICATION

While DDTC has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify the item. If doubt exists as to whether an article or service is covered by the USML, upon written request in the form of a Commodity Jurisdiction (CJ) request, DDTC will provide advice as to whether a particular article is a defense article subject to the ITAR, or a dual-use item subject to Commerce Department licensing. (22 C.F.R. § 120.4) 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.

DEFINITION OF EXPORT UNDER THE ITAR

The ITAR defines the term “Export” broadly. The term applies not only to Exports of tangible items from the U.S., but also to transfers of intangibles, such as technology or information. The ITAR defines as an “Export” the passing of information or technology to Foreign Nationals, even in the United States.” (22 C.F.R. § 120.17) The following are examples of Exports:

1. Exports of articles from the U.S. territory
    - Shipping or taking a defense article out of the United States.
    - Transferring title or ownership of a defense article to a Foreign Person, in or outside of the United States.

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

3. Export of intangibles
    - Disclosing Technical Data to a Foreign Person, whether in the United States or abroad, through oral, visual, or other means.
    - Performing a defense service for a Foreign Person, whether in the United States or abroad.

ITAR Registration

Any entity operating in the United States that either manufactures or exports Defense Articles, Defense Services, or related Technical Data, as defined in the United States Munitions List (Part 121 of the ITAR), is required to register with the Directorate of Defense Trade Controls (DDTC). Registration is primarily a means to provide the U.S. Government with necessary information on who is involved in certain manufacturing and exporting activities. Registration does not confer any export rights or privileges but is generally a precondition for the issuance of any license or other approval for export. (22 C.F.R. §§ 120.1(c) and (d); 122.1(c))

University researchers are usually engaged only in the creation of unclassified Technical Data or in the fabrication of articles for experimental or scientific purposes, including research and development. Therefore, the University is not usually required to register with DDTC. (22 C.F.R. §§ 122.1(b) (3) and (b) (4))

However, if the University desires to involve Foreign Nationals in ITAR-controlled research, it must register with the DDTC to apply for a license or take advantage of certain license exemptions. License exclusions and exemptions specific to universities are described in detail below.

Authorization to Export

Once the ITAR Registration is complete, an exporter may apply for an export authorization by submitting a relatively simple license application for the export of Defense Articles or Technical Data; or a complex license application, usually in the form of a Technical Assistance Agreement (TAA), for a complex transaction that will require the U.S. entity to provide defense services. Most types of applications also contain additional certifications or transmittal letters, supporting documentation, and in some cases, non-transfer and use certification from the licensee and/or the foreign government of the licensee.

EMBARGOED COUNTRIES UNDER DDTC REGULATIONS

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

EAR - EXPORT OF COMMERCIAL DUAL-USE GOODS AND TECHNOLOGY

BIS regulates the export of commercial products and technology under the EAR, 15 C.F.R. §§ 730-774. While there are some parallels to the ITAR, there also are some major differences in how the regulations and the relevant agencies function.

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

ITEMS CONTROLLED UNDER THE EAR

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

The EAR requires a license to Export a wide range of items with potential "dual" commercial and military use, or otherwise have strategic value to the United States (but not made to military specifications). However, only items listed on the CCL require a license prior to Export. Items not listed on the CCL are designated as EAR 99 items and generally can be exported without a license, unless the export is to an embargoed country or to a prohibited person or end-use (15 C.F.R. § 734). The following summarizes the types of items controlled under the EAR:

- Commodities. Finished or unfinished goods ranging from high-end microprocessors to airplanes to ball bearings.
- Manufacturing Equipment. This includes equipment specifically for manufacturing or testing controlled commodities, as well as certain generic machines, such as computer numerically controlled (CNC) manufacturing and test equipment.
- Materials. This includes certain alloys and chemical compounds.
- Software. This includes software specifically associated with particular commodities or manufacturing equipment, as well as any software containing encryption and the applicable source code.
- Technology. Technology, as defined in the EAR, includes both technical data and services. Unlike the ITAR, there is generally no distinction between the two.

However, the EAR may apply different standards to technology for “use” of a product than for the technology for the “design” or “manufacture” of the product.

THE COMMERCE CONTROL LIST (CCL) CATEGORIES

The CCL provides a list of very specific items that are controlled. The CCL is similar to the "dual-use" list adopted by other countries under the Wassenaar Arrangement , although the CCL has additional items. The CCL is updated from time to time, and is subject to change. The current CCL is available online at: https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

The CCL is divided into nine categories listed below:

CATEGORIES
0. Nuclear Materials, Facilities & Equipment (and Miscellaneous Items)
1. Materials, Mechanicals, Microorganisms, and Toxins
2. Materials Processing
3. Electronics
4. Computers
5. Part 1 Telecommunications
5. Part 2 Information Security
6. Sensors and Lasers
7. Navigation and Avionics
8. Marine
9. Propulsion Systems, Space Vehicles, and Related Equipment

CLASSIFICATION

Only DDTC has jurisdiction to decide whether an item is ITAR- or EAR-controlled. DDTC encourages exporters to self-classify the product. If doubt exists, a CJ request may be submitted to DDTC to determine whether an item is ITAR- or EAR-controlled.

Once it is determined that an item is EAR-controlled, the exporter must determine its ECCN. To determine EAR’s applicability and the appropriate ECCN for a particular item, a party may attempt to self-classify the item or submit a “Classification Request” to BIS. To determine whether a license is required or would be granted for a particular transaction, a party can request that BIS provide a non-binding “advisory opinion.” While BIS provides assistance with determining the specific ECCN of a dual-use item listed on the CCL, if doubt exists as to whether an item is ITAR- or EAR-controlled, BIS will stay its classification proceeding and forward the issue to DDTC for jurisdiction determination.

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

DEFINITION OF EXPORT AND RE-EXPORT UNDER THE EAR

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

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

Re-export: Similar to the ITAR, the EAR imposes restrictions on the Re-export of U.S. goods, i.e., the shipment or transfer to a third country of goods or technology originally exported from the United States.

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

AUTHORIZATION TO EXPORT

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

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

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

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

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

AT	Anti-Terrorism	CW	Chemical Weapons Convention
CB	Chemical & Biological Weapons	EI	Encryption Items
CC	Crime Control	FC	Firearms Convention

MT	Missile Technology	RS	Regional Security
NS	National Security	SS	Short Supply XP Computers
NP	Nuclear Nonproliferation	SI	Significant Items

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

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

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

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

LVS	Items of limited value (value is set under each ECCN).
GBS	Items controlled for national security reasons to Group B countries.
CIV	Items controlled for national security reasons to particular countries where end-user is civilian.
TSR	Certain technology and software to certain countries.
APP	Computer exports to certain countries.
KMI	Encryption exemption for key management.
TMP	Certain temporary exports, re-exports, or imports, including items moving through the U.S. in transit.
RPL	Certain repair and replacement parts for items already exported.
GFT	Certain gifts and humanitarian donations.
GOV	Exports to certain government entities.
TSU	Certain mass-market technology and software.
BAG	Baggage exception.
AVS	Aircraft and vessels stopping in the U.S. and most exports of spare parts associated with aircraft and vessels.
APR	Allows re-export from certain countries.
ENC	Certain encryption devices and software.
AGR	Agricultural commodities.
CCD	Authorization of certain consumer communication devices to Cuba.

License exceptions specific to universities, as well as licensing procedures, are described in detail in *Important Exclusions Applicable to University Research* below.

OFAC SANCTIONS PROGRAM AND BARRED ENTITIES LISTS

SANCTIONED COUNTRIES

U.S. economic sanctions broadly prohibit most transactions between a U.S. person and persons or entities in an embargoed country, including Iran, North Korea, Syria, and Sudan.[6] This prohibition includes the import and export 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. Because this list is not complete and subject to change, please visit http://www.treas.gov/offices/enforcement/ofac/ or http://www.treasury.gov/resourcecenter/sanctions/Programs/Pages/Programs.aspx for guidance

While most sanctions are administered by OFAC, BIS has jurisdiction over certain export prohibitions (via "embargo" regulations), as is the case with exports to Syria (15 C.F.R. § 746). In other words, a license from BIS would be required to ship most items to Syria and other OFAC-sanctioned countries or could be prohibited. Economic sanctions and embargo programs are country-specific and very detailed in terms of specific prohibitions.

TERRORIST AND OTHER BARRED ENTITY LISTS

Various U.S. Government agencies maintain a number of lists of individuals or entities barred or otherwise restricted from entering into certain types of transactions with U.S. persons. Particularly since 9/11, U.S. companies are beginning to become more assertive in attempting to place contractual terms with foreign companies related to these lists. Such lists must be screened to ensure that the University does not engage in a transaction with a barred entity. WTAMU, under a TAMU System-wide license, uses export control compliance software to expedite screening of these and other lists, including, but not limited to:

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

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

• List of Debarred Parties. The Department of State bars certain persons and entities from engaging in the Export or Re-export of items subject to the USML (available at: http://www.pmddtc.state.gov/compliance/debar.html).

Note that the number of countries subject to a U.S. arms embargo is much broader than those subject to OFAC embargoes. See http://www.pmddtc.state.gov/embargoed_countries/index.html.

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

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

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

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

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

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

OTHER RELATED REGULATIONS

Anti-Boycott Restrictions: "Participation" in such boycotts includes minor activity such as answering questions aimed at determining whether you are in violation of the boycott (e.g., whether or not you do business or have ever done business with Israel). Note that there are strict reporting requirements even where the U.S. person refuses to participate in a requested boycott action. The Anti-Boycott provisions of the EAR prohibit participation in international boycotts that have not been sanctioned by the U.S. government (e.g., the Arab League countries' boycott of Israel). See EAR Part 760 (15 C.F.R. Pt. 760).

Anti-Bribery Provisions: The Foreign Corrupt Practices Act of 1977 makes it unlawful to bribe foreign government officials to obtain or retain business.

Economic Espionage Act: makes the theft or misappropriation of a trade secret a federal crime.

Generally:

Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret:
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret:
>
> (3) Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization:
>
> (4) Attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) Conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of conspiracy:

a) Shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

b) Organizations. Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

IMPORTANT EXCLUSIONS APPLICABLE TO UNIVERSITY RESEARCH

Most university research in the United States is not subject to regulation under the EAR or ITAR based on the exclusions described below.

1. Publicly Available/Public Domain Exclusion. Information and items in the public domain, as that term is defined in 15 C.F.R. 734.3(b)(3) under the EAR; 22 C.F.R. § 120.11 under the ITAR, are not subject to control under those regulations.

a) Under the EAR, "publicly available" means:
i. Printed and published materials, prerecorded phonographic records, exposed or developed microfilm, motion picture film and soundtracks, reproducing printed and published content; or
ii. Publicly available software and technology that;
(a) Have been or will be published;
(b) Arise from Fundamental Research (see definition below); are educational; or
(c) Are included in certain patent applications.

b) Under the ITAR, "public domain" means information that is published and generally accessible or available to the public, through:
i. Sale at newsstands and bookstores, through subscriptions available without restriction, through distribution at a conference open to the public, through any patent office, and through libraries, if accessible by the public; or
ii. Public release of controlled technical data "in any form" (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency; or
iii. Fundamental Research (see definition below).

2. Fundamental Research Exclusion.

The Fundamental Research Exclusion, as set forth in both the EAR and ITAR, is pursuant to an Executive Order issued by President Reagan in 1985 and still in effect today (NSDD 189). This Order requires that: "to the maximum extent possible, the products of Fundamental Research remain unrestricted." The Order also directs that national security interests be protected through National Security Classification, not by restricting the conduct or reporting of unclassified research.

Pursuant to this Order, both the EAR and the ITAR exclude Fundamental Research from controls. Generally speaking, the Fundamental Research Exclusion applies only to information and Technical Data, and not to Controlled Physical Items.

a) Under the EAR, fundamental research means basic and applied research in science and engineering conducted by scientists, engineers, or students, at a university. Normally, university research will be considered fundamental research (and not subject to the EAR) where the resulting information is ordinarily published and shared broadly within the scientific community. However, university research is NOT considered fundamental, and therefore is subject to the EAR, if:

    i. Publication of research results is subject to restriction or withholding of research results, or substantial prepublication review, by a sponsor (other than for the protection of patents and/or sponsor's confidential proprietary information); or
    ii. The research is funded by the U.S. Government and is subject to specific access and dissemination controls.

b) Similarly, under the ITAR fundamental research means basic and applied research in science and engineering at accredited institutions of higher learning in the United States, where the resulting information is ordinarily published and shared broadly in the scientific community. However, university research will NOT be considered fundamental, and is therefore subject to the ITAR if:

    1. Publication of scientific and technical information resulting from the activity is restricted; or
    2. The research is funded by the U.S. Government and is subject to specific access and dissemination controls.

3. ITAR Exclusion for Educational Information. The ITAR specifically excludes from regulation information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, or universities. Such educational information is not included as part of the "Technical Data" that is subject to ITAR controls.

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

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

- will ship or hand-carry the items, technology, or software for WTAMU business only;
- will return or certify the destruction of the items, technology, or software within twelve (12) months of leaving the U.S.;
- will keep the items, technology, or software within his or her effective control;
- will take necessary security precautions to protect against the unauthorized export of the technology; and
- will not ship or hand-carry the items, technology, or software to Iran, Syria, Cuba, North Korea, or Sudan without first consulting with WTAMU's Empowered Official.

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

- The technical data is to be used overseas solely by a U.S. person(s);

- The U.S. person overseas is an employee of WTAMU or the U.S. Government and is not an employee of a foreign subsidiary;
- If the information is classified, it will be sent overseas in accordance with the requirements of the Department of Defense Industrial Security Manual; and
- No export will be made to countries listed by 22 C.F.R. § 126.1.

5. ITAR Registration Exemptions. The ITAR exempts certain persons and entities from the registration requirement, including "Persons who engage only in the fabrication of articles for experimental or scientific purpose, including research and development." However, ITAR Registration is generally a precondition to the issuance of any license or other ITAR approval. (22 C.F.R. § 122.1)

EXCEPTIONS TO UNIVERSITY TRAVEL

WTAMU employees and students traveling outside the U.S. intending to bring laptops or other data storage equipment must ensure that there is no export-controlled information contained on such devices unless there is a specific license or other authorization in place for that information for that destination. Any individual intending to travel or transmit controlled data outside the U.S. should first consult with the Empowered Official or SRS.

It is important to note that activities involving teaching or training Foreign Persons on how to use equipment may require a license.

The pertinent exceptions include:

1. Export License Exception (TMP). The export of items, technology, commercial software, and encryption code is subject to export control regulations (this includes laptops, PDAs and digital storage devices). EAR makes an exception to licensing requirements for the temporary Export or Re-export of certain items, technology, or software for professional use as long as the criteria below are met. The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products. In addition, this exception does not apply to items, technology, data, or software regulated by ITAR.

2. Export License Exception (Bag or Baggage). EAR makes an exception to the licensing requirement for the temporary Export or Re-export of certain items, technology, or software for personal or professional use as long as the criteria to which one certifies below are met. The exception does not apply to any EAR satellite or space-related equipment, components, or software, or to any technology associated with high-level encryption products. It also does not apply to ITAR items, technology, data, or software.

WTAMU faculty, staff, or students should not ship or hand-carry controlled items, technology, or software to any country on OFAC's Sanctions Program and Country Summaries list, (see http://www.treasury.gov/resourcecenter/sanctions/Programs/Pages/Programs.aspx) without first consulting with the Empowered Official or SRS.

3. Laptop (TAMU-owned) Baggage Exception. Faculty, staff, and students who need to take their laptops out of the country in connection with University fundamental research may do so under the baggage exception for temporary export as long as:

   - the country of travel is not under U.S. sanctions;
   - the laptop is a "tool of trade;" and
   - the laptop remains in their possession and control at all times.

Please note that other exceptions or exemptions may be available.

RECORD KEEPING

1. ITAR Requirements. If ITAR-controlled Technical Data is Exported under an exemption, certain records of the transaction must be kept even beyond WTAMU's seven (7) year retention period. (22 C.F.R. §§ 122.5 and 123.26) Those records include:

- A description of the unclassified technical data;
- The name of the recipient/end-user;
- The date/time of export;
- The method of transmission (e.g., email, fax, telephone); and
- The exemption under which the export took place.

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

2. EAR Requirements. BIS have specific recordkeeping requirements. Generally, records required to be kept by EAR must be kept for a period of five (5) 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.

3. OFAC Requirements. Generally, OFAC requires that records be available for examination for at least five (5) years after the date of any transaction that is subject to the regulations. Except as otherwise provided in the regulations, every person holding blocked property is required to keep a full and accurate record of such property for at least five (5) years after the date such property is unblocked. (31 C.F.R. § 501.601)

Appendix B – Contract Provisions of Concern

Most data and information involved in University research is excluded from export control regulation under the ITAR or EAR based on several key provisions:
(a) The Public Domain Exclusion;
(b) The Fundamental Research Exclusion (FRE); and
(c) The Exclusion for Educational Information.

The aforementioned provisions are more fully described in this Appendix. It is important for researchers and others involved in research to be aware of these key exclusions and to understand that their benefits can be lost if certain provisions are present in research-related agreements. For this reason, PIs should avoid entering into informal understandings or "side agreements" with research sponsors that restrict Foreign Person access to the research or that impose sponsor controls on the publication or other dissemination of research results. It is important to remember that the restrictions enforced by OFAC are not affected by ITAR, EAR, or the FRE.

1. Contract Provisions of Concern

Certain research agreement provisions may negate the FRE and require seeking a license or undertaking monitoring or other activities. These provisions of concern are summarized below. If any of the following provisions are present (and cannot be negotiated out) in a research agreement or subagreement, a Material Transfer Agreement (MTA), or Non-Disclosure Agreement (NDA) related to research, the agreement will trigger a secondary screening and should be submitted for SRS:

a) Sponsor maintains the right to restrict or approve publication or release of research results (other than WTAMU's standard customary brief delay to protect a sponsor's confidential information or to preserve the patentability of an invention).

b) Research data and/or other research results will be owned by the sponsor (e.g., as sponsor's proprietary or trade secret information).

c) Statements that export control regulations will apply to the research.

d) Incorporation by reference of Federal Acquisition Regulations (FARs), agency specific FARs, or other federal agency regulations, which impose specific controls on access to or dissemination of research results (see Section 1.2 below).

e) Restrictions on, or prohibitions against, the participation of research personnel based on citizenship or national origin.

f) Statements that the sponsor anticipates providing export-controlled items or information for use in connection with the research.

g) Equipment or encrypted software is required to be delivered as part of the project.

h) The research project will involve the use of export-controlled items or technical information obtained from a third party.

i) The research will take place outside the United States.

j) The research is funded by a non-US sponsor.

1.2 Specific U.S. Government Access and Dissemination Controls

Specific access and dissemination controls may be buried within the language of FARs, Defense Federal Acquisition Regulations (DFARs), and other agency-specific regulations included as part of a prime contract, or flowed down in a subcontract.

These problematic clauses include, but are not limited to:

FAR 52.227-14 (Rights in Data - General).

Grants the Government unlimited rights in data first produced or delivered under the contract. Government approval required to assert copyright in data first produced in the performance of the contract and not published in academic, technical or professional journals, symposia proceedings, or similar works. For basic or applied research suggest requesting Alternate IV to lift this restriction. Alternate IV provides the Contractor with the right to copyright data without Government permission.

FAR 52.227-17 (Rights in Data - Special Works).

Prevents the release, distribution, and publication of any data originally produced in the performance of the award. This establishes controls for data generated by contractors for the Government's internal use and represents an absolute restriction on the publication or dissemination of contractor-generated data. It should not apply to basic and applied research and should be removed from the contract on the basis of exceptions to this clause's applicability. Refer to FAR 27.405(a)(1).

DFAR 252.204-7000 (Disclosure of Information).

States, "Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract." Three exceptions apply: (1) if the contracting officer has given prior written approval; (2) where the information is already in the public domain prior to date of release; (3) if the research is determined in writing to be fundamental research by the Contracting Officer.
Refer to 27.404-2 & 27.404-3 and NSDD-189 as justification for getting the restriction removed. Also, can refer to IRS Ruling 76-296. May also add alternate language that allows for review and comment on publications.

DFAR 252.204-7048 (Export-Controlled Items).

States, "The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR." May have to require the PI to certify that the project does not involve any items that are subject to Export Control Laws.

ARL 52.004-4400 (Approval of Foreign Nationals).

All Foreign Nationals must be approved before beginning work on the project. Contractor is required to divulge if any Foreign Nationals will be working on the project. Provision of name, last country of residence, citizenship information, etc. is required. This clause is commonly found in contracts involving Controlled Technology and sponsored by military agencies. May need to require the PI to certify that no Foreign Nationals will be working on the project. If no Foreign Nationals will be employed on the project, Contractor may disregard this clause. If no Foreign Nationals will be employed on the project, the clause may be disregarded. If the PI is doing basic research and the sponsor will take those results and work on the controlled technology at another location, may be able to delete this clause.

ARL 52.005-4401 (Release of Information).

Includes reference to “non-releasable, unclassified information” and a requirement to “confer and consult” with the sponsor prior to release of information. The sponsor retains publication/information approval, which voids the FRE. Substitute with ARL Cooperative Agreement Language: Prior Review of Public Releases, “The Parties agree to confer and consult with each other prior to publication or other disclosure of the results of work under this Agreement to ensure that no classified or proprietary information is released. Prior to submitting a manuscript for publication or before any other public disclosure, each Party will offer the other Party ample opportunity (not to exceed 60 days) to review such proposed publication or disclosure, to submit objections, and to file application letters for patents in a timely manner.”

AFMC 5352.227-9000 (Export-Controlled Data Restrictions).

Requires an export license prior to assigning any Foreign National to work on the project or allowing Foreign Nationals access to the work, equipment, or technical data generated by the project. Foreign Nationals make up a portion of WTAMU’s scientific undergraduate, graduate, and visiting scholar population. Often, it is difficult to find qualified U.S. citizens to work on these projects. Also, many students depend on these projects to complete their thesis or dissertation. Need to ask the PI if the project is basic or applied research. If yes, it may fall under an ITAR exclusion. May also ask the defense contractor if foreign students are allowed to work on the project. If yes, obtain confirmation in writing.

DFAR 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting).

The Contractor shall provide the security requirements described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, and when the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall – Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts, and rapidly report all cyber incidents to DoD at http://dibnet.dod.mil.

1.3 Procedures Applicable to Research Agreements and Subcontracts

1.3.1 Proposals

Based on proposal timing and the limited information available at proposal submission, limited screening may be conducted by SRS at this stage.

1.3.2 Agreements and Subcontracts

(a) *Restricted Party Screening*
If RPS has not been conducted at the proposal stage, SRS will conduct RPS of non-federal sponsor(s) and/or subcontractor using the screening software licensed by WTAMU. A record of the screening results will be maintained as part of the project files. Issues that cannot be resolved by SRS will be referred by SRS to TAMUS ORC and/or OGC as appropriate for a determination prior to release of funds.

(b) *Contract Provisions of Concern*
Agreements and subcontracts will be reviewed by SRS to identify restrictions that may negate the FRE or other exclusions identified in TAMUS Policy 15.02, Export Controls. If any such restrictions are present (and cannot be negotiated out), SRS will work with the PI as appropriate to address the export control compliance concern. Issues that cannot be resolved will be referred by the Export Control Officer to TAMUS ORC and/or OGC as appropriate.

1.4 Determining EAR or ITAR Commodity Jurisdiction

1.4.1 If an agreement or subcontract includes contract provisions of concern, the PI will work closely with the Export Control Officer in providing the required information. The PI will refer to the ITAR US Munitions List, 22 C.F.R. 121.1 http://www.fas.org/spp/starwars/offdocs/itar/p121.htm, the EAR Commerce Control List, 15 C.F.R. Part 738, Supplement 1 to Part 738 http://www.access.gpo.gov/bis/ear/pdf/738spir.pdf, and other relevant parts of the regulations as directed by the Export Control Officer, to identify the appropriate export classification.

1.4.2 A determination of commodity jurisdiction will be made by the Export Control Officer and will be documented for the PI. The SRS will also undertake further export control analysis pursuant to Section 1.5 *Resolving Export Control Issues* of this Manual.

1.4.3 If the Export Control Officer, with the assistance of the PI, is not able to make a commodity jurisdiction determination, the Export Control Officer will consult with TAMUS ORC and/or the OGC. If there is still a question about commodity jurisdiction, the Export Control Officer will prepare a commodity jurisdiction request for submission to the Department of State or a commodity classification request to the Department of Commerce, as appropriate. In such cases, until an official determination is received, the project will be considered export-controlled, and no Foreign Persons will be permitted to participate until an official determination is made to the contrary. Requesting an official commodity jurisdiction ruling from the government takes time. A minimum of two weeks is required for completion of the request itself, and several more weeks can be expected before the receipt of a response from the government.

1.4.4 Finalization of the agreement or subcontract need not be delayed pending SRS's determination of commodity jurisdiction or other export control issues; however, all necessary controls must be implemented before the work begins.

1.5 Resolving Export Control Issues

1.5.1 Office of Research Compliance

Once a potential export control issue is identified, the Export Control Officer and/or the Empowered Official will work with the parties involved, as appropriate, and determine what course of action should be taken to address the issue. In many cases, no license or other authorization may be necessary. In each case, the Export Control Officer and/or the Empowered Official will determine whether:

(a) The conditions merit an application for a license or other authorization,

(b) The conditions are such that an exclusion or license exception may be obtained, or

(c) A TCP, or other requirements for the conduct of the research, will be necessary to prevent an unauthorized Deemed Export of the technology from occurring.

The Export Control Officer will notify the PI of the export control determinations and will maintain records of its determinations on a project basis, as provided in Section 5 *Recordkeeping*.

1.5.2 Technology Control Plan

1.5.2.1 Development

If the Export Control Officer and/or the Empowered Official determines a project or facility is export-controlled, the Export Control Officer will work with the PI to develop and implement a TCP to secure the Controlled Technology from access by unauthorized Foreign Persons. A TCP will typically include:

(a) A commitment to export controls compliance;

(b) Identification of the relevant export control categories and Controlled Technologies;

(c) Identification of the project's sponsors;

(d) Identification and nationality of each individual participating in the project;

(e) Appropriate physical and informational security measures for the duration of the project;

(f) Personnel screening measures and training; and

1.5.2.2 Appropriate Security Measures

The TCP will include physical and informational security measures appropriate to the export control categories involved on the project.

Examples of security measures include, but are not limited to:

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

(b) **Time Blocking.** Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access.

(c) **Marking.** Export-controlled information must be clearly identified and marked as export-controlled.

(d) **Personnel Identification.** Individuals participating on the project may be required to wear a badge, special card, or other similar device indicating authority to access designated project areas. Physical movement into and out of a designated project area may be logged.

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

(f) **Electronic Security.** Project computers, networks, and electronic transmissions should be secured and monitored through User IDs, password controls, 128-bit Secure Sockets Layer encryption, or other federally approved encryption technology. Database access should be managed via a Virtual Private Network (VPN).[7]

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

4.5.3 Export Licensing

If a license, Technical Assistance Agreement, Manufacturing License Agreement, ITAR Registration, or other authorization is the appropriate method as determined by the Export Control Officer and/or the Empowered Official to address an export control issue, the Export Control Officer and/or the Empowered Official will consult with the PI and other appropriate parties to gather all the information needed to submit the appropriate

[7] A mechanism for providing secure, reliable transport over the Internet. A VPN uses authentication to deny access to unauthorized users, and encryption to prevent unauthorized users from reading the private network packets. The VPN can be used to send any kind of network traffic securely, including voice, video or data.

documentation to seek a license. The Empowered Official will request the license or other authorization from the cognizant agency with assistance from TAMUS ORC and the OGC as appropriate.

Appendix C – Export Control Forms

International Visitors Screening Form – Restricted Party Screening Form (2 pages)

Shipping Form – WTAMU Export Controls Confirmation Form for International Shipments

Visual Compliance User Form – All users are limited to U.S. citizens and legal permanent residents who are full-time employees of WTAMU.

Technology Control Plan (TCP) and Amendment Form – Used to secure Controlled Technology

Restricted Party Screening Form – Page 1

BACKGROUND: In accordance with ***University Rule 15.02.99.W1 Export Controls*** international visitors intending to visit WTAMU must undergo a restricted party screening as a pre-condition of their visit to WTAMU.

This includes all invited International Visitors whether or not currently present in the United States.

It is the responsibility of all employees at WTAMU who intend to host an international visitor to notify and request approval of such visit form the Export Control Officer before the arrival of the international visitor.

INSTRUCTIONS: Complete the 2 page form below for **each** international visitor and the entity they either represent or are employed by. Forward the completed form to exportcontrol@wtamu.edu. Please allow a minimum of 3 working days for the screening to be completed. If additional information is necessary to complete the screening you will be contacted. Results of the restricted party screening will be sent to you via email. Contact Janet Wood, the Export Control Officer, at 651-2982 / jawood@wtamu.edu with any questions.

INTERNATIONAL VISITOR

Name: _____ Date of Birth: _____

Address: _____ Citizen of: _____

City/State: _____

Country: _____

COMPANY OR INSTITUTION BEING REPRESENTED

Name: _____

Address: _____

City/State: _____

Country: _____

Date of Visit:

Locations to be Visited:

WTAMU Point of Contact:

WTAMU POC email/phone:

Purpose of Visit:

Restricted Party Screening Form – Page 2

The following questions are intended to address export controlled issues. Please check "yes" or "no" for all of the work contemplated during the visit, both funded work and unfunded work, with the host or other faculty member or researcher.

YES	NO	QUESTION
		Will visitor have access to research which could categorized as Classified? Classified research is usually government funded and can further be defined as national security information at the levels of Top Secret, Secret, and Confidential, and as being governed by Department of Defense National Industrial Security Program Operating Manual (NISPOM) requirements. Publication of classified research results can be legally withheld or restricted.
		Will visitor have access to research which could be categorized as Controlled Unclassified Information? Controlled Unclassified Information (CUI) is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the US or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU)
		Will visitor have access to research categorized as Proprietary? Proprietary research, usually privately funded, is defined as research activities undertaken pursuant to a contract between the University and an outside sponsor with commercial interests, and carried out under the auspices of the University. Publication of proprietary research results can be withheld or restricted, contractually.
		Will visitor have access to projects which restrict participation to US citizens or permanent residents only?
		Will visitor have access to research categorized as Restricted? Restricted research is research where publication may require advance review by, or permission of the funding entity. Restricted research may have constraints imposed by the funding entity, whether it be the state, a federal agency, or a private sponsor with or without commercial interests.
		Will visitor have access to research categorized as "Fundamental"? Fundamental research means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons. Fundamental Research applies only to the dissemination of technical data and information, not to the transmission of material goods.
		Will visitor have access to technical specifications of equipment where such specifications are not available through published materials such as commercially available manuals, documentation in libraries or the World Wide Web, information from teaching laboratories or information available to interested communities for either free or where the price does not exceed the cost of production.

HOST FACULTY MEMBER: _____

Print or type name

_____ Date: _____

Signature

WTAMU Export Controls Confirmation Form for International Shipments

This form MUST accompany ALL International Shipments. A "Yes" response to any of the four questions below requires a description and export control authorization before shipment: FAX TO: Randy Brown, Central Receiving, FAX #806-651-2109

1) Yes / No
Does the shipment contain items, information, or software on the U.S. Dept. of Commerce Control List (CCL: http://www.bis.doc.gov/policiesandregulations/ear/index.htm); or is it being shipped to an entity or person in a country subject to US economic or trade sanctions or identified by the US Department of State as a "State Sponsor of Terrorism" (https://www.state.gov/j/ct/list/c14151.htm) , namely Iran, Sudan, Syria or North Korea?

2) Yes / No
Are you shipping, transmitting, or transferring developed, non-commercial encryption software in source code or object code?
(Note: Most publicly available "dual-use" encryption code captured by the Export Administration Regulations (EAR) requires the availability of a License Exception. A License Exception under the EAR is an authorization based on a set of criteria, which when met, allows the exporter to circumvent export licensing requirements. The release of publicly available encryption code under the EAR is generally authorized by License Exception TSU (Technology and Software - Unrestricted) whereby the exporter provides the US Government with a "one-time" notification of the location of the publicly available encryption code prior to or at the time the code is placed in the public domain. Notification after transmission of the code outside the US is an export control violation.)

3) Yes / No
Does the shipment contain items, information, or software that could support the design, development, production, stockpiling or use of a nuclear explosive device, chemical/biological weapons, missiles, a defense article, or technical data on the ITAR's US Munition List (USML)?
(Note: USML ITAR Part 121: https://www.gpo.gov/fdsys/granule/CFR-2012-title22-vol1/CFR-2012-title22-vol1-part121 ; US persons are specifically prohibited from engaging in activities, either directly or indirectly, that support the proliferation of nuclear explosive devices and missiles to certain countries and their nationals without an export license. Certain chemical and biological weapons agents and precursors are listed on the US Munitions List (USML) and on the Commerce Control List (CCL).)

4) Yes / No
Does the shipment contain items, information, or software under a Non-Disclosure Agreement, a Confidentiality Agreement, or a sponsored agreement imposing publication restrictions beyond a brief review (up to 90 days) for patent protection and/or inadvertent release of confidential/proprietary information?
(Note: Non-Disclosure Agreement (NDA) may include licensing agreements which limit or prohibit the disclosure or transfer of the licensed data or materials. If the confidential data pertains to such information as personal health, income, or other demographic data that does not have a strategic significance, and is thus not identified on US export control lists, then export control restrictions would not apply.)

I certify that the packaged international shipment described above complies with Texas A&M University System Policy #15.02 – Export Controls, West Texas A&M University's Export Controls Rule, and all other federal laws and regulations regarding export controls.

_____ _____

Signature Date

For questions or additional information please contact:

Janet Wood
West Texas A&M University Export Control Officer
#806-651-2982; jawood@wtamu.edu

Zack Workman
West Texas A&M University Risk Management
#806-651-2961; Fax #806-651-2096

TEXAS A&M University Export Control Office

Request to Activate/Deactivate Access to Export Control Compliance Software

This form should be completed by the Texas A&M University department/unit head, or by the System member's export control representative, as appropriate, and signed and submitted to TAMU's Export Control Office. A signature is also required from the proposed user if this is a request for a new account.

SECTION A

( ) Deactivate Account(s)* Please specify account name(s) _____.

Please deactivate the account(s) listed above effective _____201__.

Requesting Department/Unit/System Member Export Control Representative:

_____ (signature)
Name: _____
Title: _____
Dated: _____

*Account deactivation means that the searches of the existing account user will continue to remain accessible to the System member.

SECTION B

( ) Activate New Account. Complete Section B.

1. My department/unit/system member export control office has completed a restricted party screening of the proposed user using export control compliance software licensed by Texas A&M University known as Visual Compliance ("Software"). The results of the screening did not raise concerns that have not been discounted as false positives.

   Yes: ___ No: ___

   By marking the "no" box, I am requesting that TAMU's Export Control Office perform restricted party screening of the proposed user, because there has been no prior screening of the proposed user.

2. The proposed user is a U.S. citizen or a U.S. legal permanent resident.

3. My department/unit has implemented written internal procedures relating to use of the Software.

4. The proposed user has a business need to use and access the Software.

5. The proposed user has completed the basic on-line export control training course made available on The Texas A&M University System website.

6. The proposed user will complete supplemental training as directed by TAMU's Export Control Office, including training in the use of the Software.

7. If the proposed user's employment responsibilities or status changes, so that use and access to the Software is no longer necessary or appropriate, the requesting department/unit head/system member export control representative is responsible for providing prompt notice to TAMU's Export Control Office.

8. The proposed user will use the Software in accordance with applicable System and Texas A&M University policies, regulations, rules and procedures; and will use the Software only as needed to conduct West Texas A&M University/Texas A&M University System business.

By signing this request, I certify that all information found in this request is accurate to the best of my knowledge, and I have read and agree to the above terms.

Proposed User:

First Name	Last Name	Title
Email	Telephone	Address
City	State	ZIP Code
Signature	Date	

Requesting Department/Unit/System Member Export Control Representative:

_____
(signature)

Name: _____

Title: _____

Dated: _____

Technology Control Plan

Development

If the Export Control Officer (ECO) determines a project, facility, or item is export-controlled, the ECO will work with the PI, facility managers, and others, as appropriate, to develop and implement a Technology Control Plan (TCP) to secure the Controlled Technology from access by unauthorized Foreign Persons. A TCP will typically include:

(a) A commitment to export controls compliance
(b) Identification of the relevant export control categories and controlled technologies
(c) Identification of the project's sponsor(s)
(d) Identification and nationality of each individual participating in the project
(e) Appropriate physical and informational security measures
(f) Personnel screening measures and training
(g) Appropriate security measures for the duration of the project through project termination

Appropriate Security Measures

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

(a) Laboratory Compartmentalization. Project operation may be limited to secured laboratory areas physically shielded from access or observation by unauthorized individuals. These areas must remain locked at all times.
(b) Time Blocking. Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access.
(c) Marking. Export-controlled information must be clearly identified and marked as export-controlled.
(d) Personnel Identification. Individuals participating on the project may be required to wear a badge, special card, or other similar device indicating authority to access designated project areas. Physical movement into and out of a designated project area may be logged.
(e) Locked Storage. Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key controlled access. Soft and hardcopy data, lab notebooks, reports, and other research materials should be stored in locked cabinets.
(f) Electronic Security. Project computers, networks, and electronic transmissions should be secured and monitored through User IDs, password controls, 128-bit Secure Sockets Layer encryption, or other federally approved encryption technology. Database access should be managed via a Virtual Private Network.
(g) Confidential Communications. Discussions about the project must be limited to the identified and authorized project participants, and only in areas where unauthorized individuals are not present. Discussions with third party subcontractors must occur only under signed agreements which fully respect the Foreign Person limitations for such disclosures.

West Texas A&M University
Technology Control Plan

Statement of Commitment

West Texas A&M University is committed to export control compliance. It is the policy of West Texas A&M University to comply with United States export control laws and regulations. All employees and students must be aware of and are responsible for the export control implications of their work and must ensure that their activities conform to export control laws and regulations. Individuals and the university may be subject to severe penalties for violations of export control laws and regulations, including the loss of research funding, loss of export privileges, as well as criminal and civil penalties.

This project/activity/equipment involves or has the potential to involve the receipt and/or use of Export-Controlled Items, Technology, or Information. As a result, the project/activity comes under the purview of either the State Department's International Traffic in Arms Regulations (ITAR)(22 CFR Parts 120 – 130) or the Department of Commerce's Export Administration Regulations (EAR) (15 CFR §§734.8 and 734.9) and/or other export control regulations.

Export-controlled technical information, data, items, software, hardware, biological, and chemicals must be secured from use and/or observation by unauthorized foreign nationals.

In accordance with U.S. export control laws and regulations, a Technology Control Plan (TCP) is required to prevent unauthorized access and/or use of export controlled items, information, technology or software. This document serves as a basic template for the minimum elements of a TCP and the safeguard mechanisms to protect against unauthorized access or use. Security measures and safeguards shall be appropriate to the export classification. Contact the West Texas A&M Export Controls Office at (806)651-3554 or (806)651-2982 for assistance to complete this form.

Establishing a TCP is a multi-step process. The first step is the assessment and approval phase where the principal investigator/responsible individual ("PI") develops a TCP in coordination with West Texas A&M's Export Controls Office and seeks approval of the plan from the PI's department/unit head, and West Texas A&M's Export Controls Office. When all approvals have been secured the PI shall review the TCP with all users, and each user will sign a copy of the briefing and certification form at the end of the TCP outlining individual responsibilities for handling export controlled technology, information and/or items. When all users, including the PI, have signed the TCP briefing and certification, the PI submits all signed documents to West Texas A&M's Export Controls Office, retains copies for their files, and implements the TCP. It is the PI's responsibility to notify West Texas A&M's Export Controls Office of any anticipated changes to the TCP (e.g., personnel, scope of work, safeguards, etc.). All records relating to TCPs will be retained for at least five years from the TCP closure date or at least five years beyond the date it becomes no longer necessary to protect covered items, technology and/or information. Records will be maintained in accordance with the Texas A&M record retention policy, 15 C.F.R., Part 762 (EAR); 22 C.F.R. §§122.5, 123.22, 123.26 (ITAR); and 31 C.F.R. §501.601 (OFAC).

Title of Project or Activity: (describe project, activity or equipment subject to TCP)
Click or tap here to enter text.

Identification of sponsor and relevant project number:
Click or tap here to enter text.

Description of Export Controlled Item, Technology, Information or Software and reason for control:
Click or tap here to enter text.

Principal Investigator/Responsible Individual: Last, First
Phone: Click or tap here to enter text.
Email: Click or tap here to enter text.

Identified Export Control Classification Number / ECCN: (e.g. 5D002) <OR> ITAR Category: (e.g. VII (e))
If you do not have the ECCN or ITAR Category, contact your sponsor or program manager for this vital information. This form cannot be processed without the applicable ECCN or the ITAR Category. Click or tap here to enter text.

Briefing Requirement
The Principal Investigator/Responsible individual is required to brief his or her staff on the requirements of this TCP.

1. Physical Security Plan: (Data and/or items, technology must be physically shielded in secured lab spaces to prevent observation or possession by unauthorized individuals or during secure time blocks when observation by unauthorized persons is prevented. This would pertain to laboratory management of "work-in-progress".)

Location (include building and room numbers, lab name, etc.):
Click or tap here to enter text.

Physical Security (provide a description of your physical security plan designed to protect the item/technology from unauthorized access or unauthorized removal of technical information, data, items, software, hardware, biological and chemicals (e.g. secure doors, limited access, security badges, locked desks or cabinets, secure computers, marking all physical items etc.):
Click or tap here to enter text.

Item Storage (Both soft and hard copy data, notebooks, reports and research materials are stored in locked cabinets; preferably in rooms with key-controlled access. Equipment or internal components and associated operating manuals and schematic diagrams containing "export-controlled" technology are to be physically secured from unauthorized access):
Click or tap here to enter text.

Servicing of item (provide a description of how this item will be serviced or repaired during its lifetime and how custodial and related services will be addressed, including disposal and destruction):
Click or tap here to enter text.

Janitorial Service (provide a description of how this item will be secured during custodial servicing periods):
Click or tap here to enter text.

2. Information Security Plan (Appropriate measures must be taken to secure controlled electronic information, including User ID's, password control, SSL etc.)

Describe what information security safeguards will be used:
Click or tap here to enter text.

3. Amendments: Any changes to the approved plan, including personnel changes and location changes, must be approved in writing. Please submit a completed TCP Amendment Form as needed.

4. Personnel (clearly identify every person who may have access to the controlled information, technology or item) *(Use Tab key to maneuver throughout table and to add rows)*

Last Name	First Name	Citizenship	Date of Birth

Any change (removal or addition) in personnel will require an amendment of this plan. On departure of any personnel listed above, appropriate measures must be implemented to secure the subject matter of the TCP. This includes collecting all keys, removing swipe card access, and updating access controls.

5. Personnel Screening Procedures: All persons who may have access to export-controlled items, information and/or technology must be listed on the TCP and undergo Restricted Party Screening using export control screening software licensed by West Texas A&M. **Screening Results will be maintained as part of this TCP.**

6. Training / Awareness Program
All participants listed on a TCP must complete export control online basic training, sign the Certification for Safeguarding Export Controlled Technology, Information or Items, and be briefed by the PI/Responsible Individual as to the restrictions of this TCP. Additional training is recommended for all individuals listed; please contact the West Texas A&M Export Controls Office at (806)651-2982 or (806)651-3554 to schedule additional training.

(Use Tab key to maneuver throughout table and to add rows)

Last Name	**First Name**	**Date Export Control Training Completed**

7. By signing this TCP, I certify that I have read and understand all clauses found in this TCP. I certify that all information found in this TCP is accurate and complete to the best of my knowledge.

Principal Investigator / Responsible Individual

Signature _____ Title _____

Printed Name _____ Date _____

Department/Unit Head

Signature _____ Title _____

Printed Name _____ Date _____

8. Reviewed By:

Signature _____ Title _____

Printed Name _____ Date _____

WEST TEXAS A&M UNIVERSITY

Technology Control Plan Briefing and Certification on the Handling of Export-Controlled Information, Items, Technology and Software

**Upon authorization of your TCP, complete this form for each person who will have access to the export controlled information, technology, software, or items. Send copies of the completed forms to the Export Control Office via email srs@wtamu.edu.*

BACKGROUND

The subject matter of the Technology Control Plan (TCP) identified below may involve the use of export-controlled information, technology, items or software. The International Traffic in Arms

Regulations (ITAR), enforced by the Department of State, and the Export Administration Regulations (EAR), enforced by the Department of Commerce, prohibit sending or taking export controlled information, items, technology or software out of the U.S. and disclosing or transferring export-controlled information to a Foreign Person inside or outside the U.S. Verbal and visual disclosures are equally prohibited.

- A Foreign Person is defined as any person who is not a U.S. citizen or legal permanent resident of the U.S. There are no exceptions for foreign graduate students or visiting scholars.

Generally, export-controlled means that the information item,, technology and software related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use items with a capacity for substantial military application utility requires an export license, or license exception, before it may be physically exported or discussed or disclosed to a Foreign Person. Export-controlled information does not include basic marketing information about function or purpose, general system descriptions, or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain. It does not matter whether the actual intended use of export-controlled information is military or civil in nature.

PARTICIPANTS RESPONSIBILITIES

Participants may be held personally liable for violations of the EAR and the ITAR, with significant financial and criminal penalties as a result. With that in mind, it is extremely important that Participants exercise care and caution in using, disclosing or transferring export-controlled information, items, technology or software with others inside the U.S. and outside without prior authorization from the appropriate federal agency. For example, Participants must identify who among proposed research project personnel and collaborators are Foreign Persons. If a Foreign Person does not have security clearance, the State Department or the Department of Commerce (depending on whether the ITAR or the EAR controls the technology) must grant a license authorizing that person access to export-controlled information. Participants must secure access to export-controlled information, items, technology or software to prevent unauthorized access or use. They must clearly identify export-controlled information, items, technology or software and make copies of export controlled information only when absolutely necessary. Participants must securely store export-controlled information in locked filing cabinets, locked drawers, or under password protected computer files. Participants shall avoid moving export-controlled information from one location to another, if at all possible.

CRIMINAL/CIVIL LIABILITY AND PENALTIES

The penalty for unlawful export and disclosure of export-controlled information under the ITAR is up to two (2) years imprisonment and/or a fine of one hundred thousand dollars ($100,000). The penalty for unlawful export and disclosure of information controlled under the EAR is the greater of either a fine of up to one million dollars ($1,000,000) or five (5) times the value of the exports for a corporation and imprisonment of up to ten (10) years and/or a fine of up to two hundred fifty thousand dollars ($250,000) for an individual. *It is very important to remember that individuals may be held personally liable for export control violations even when performing a project that is funded through the University.*

Principal Investigator/Responsible Official: _____
Department/Unit: _____
Title of Project/Activity:_____
Technology Control Plan Number: _____

CERTIFICATION

- I hereby certify that I have read and understand this Briefing and Certification. I understand that I could be held personally liable if I unlawfully allow access to or disclose, regardless of form or format, export-controlled information, technology, software, or items to unauthorized persons.

- I understand that the law makes no specific exceptions for non-US students, visitors, staff, postdocs or any other person not pre-authorized under a TCP to access export controlled information, technology, software or items.

- I also acknowledge that I have read the West Texas A&M University Technology Control Plan for this project/activity and have discussed the plan with my supervisor (if not the PI / Responsible Individual) and that I agree to comply with the requirements in the TCP.

- Furthermore, I have taken the University's Export Control Training as set forth in the TCP and as prescribed by University Rule 15.02.99.M1 *Export Controls.* I agree to immediately contact the West Texas A&M Export Controls Office at (806)651-3554 or (806)651-2270, with any questions I may have regarding the designation, protection, or use of export-controlled information, technology, software, or items.

Participant Name:	Participant Signature:	Date:

Technology Control Plan Amendment Form

Instructions

Submit this form to amend an approved Technology Control Plan. Amendments may include changes in the physical security plan (location of covered items, servicing or maintenance, or changes in item security), changes to the information security plan, and/or changes to authorized personnel. Please provide sufficient detail describing the requested changes, including justification.

TCP Number: Click or tap here to enter text.
Principal Investigator/Responsible Individual: Last, First
Phone: Click or tap here to enter text.
Email: Click or tap here to enter text.

Indicate all areas of the TCP modified by this amendment:

☐Physical Security Plan	☐Information Security Plan	☐Personnel

1. Physical Security Plan

Click or tap here to enter text.

2. Information Security Plan

Click or tap here to enter text.

3. Addition of Authorized Personnel

Last Name	First Name	Citizenship	Date of Birth

Training Verification (Must be included for any personnel additions)

Last Name	First Name	Date Export Control Training Completed

4. Technology Control Plan Briefing and Certification on the Handling of Export-Controlled Information, Items, Technology and Software form must be reviewed and signed by all new personnel. Include signed forms with this amendment submittal.

5. Removal of Authorized Personnel

Last Name	First Name	Citizenship	Date of Birth

6. Principal Investigator / Responsible Individual:

By signing this TCP Amendment, I certify that I have read and understand all clauses found in this Amendment. I certify that all information found in this TCP Amendment is accurate and complete to the best of my knowledge.

Principal Investigator Signature:	
Printed Name:	Date:

6. Reviewed By:

Signature:	
Printed Name:	Date:
Title:	

Appendix D – Glossary of Terms

Definitions

Controlled Information - Information about Controlled Physical Items, including information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of Controlled Physical Items and may be released through visual inspection, oral exchanges, or the application of personal knowledge or technical experience with Controlled Physical Items. It also includes information in the form of blueprints, drawings, photographs, plans, instructions, and documentation. Further included in this definition are non-physical items (software and algorithms, for example) listed under EAR and ITAR. (See 15 CFR 730-774 and 22 CFR 120-130 for further details.)

Controlled Physical Items – Controlled Physical Items are dual-use technologies listed under the EAR and defense articles listed on ITAR's USML. (See 15 CFR 730-774 and 22 CFR 120-130 for further details.)

Deemed Export–The transfer of Controlled Information or Controlled Physical Items, or the provision of defense services to a Foreign Person in the United States is deemed to be an Export to the home country or countries of the Foreign Person, and is subject to the export control laws and regulations.

ECCN – The Export Control Classification Number (ECCN) is the number assigned to each specific category of items or technology listed specifically on the Commerce Control List (CCL) maintained by the U.S. Department of Commerce, Bureau of Industry and Security (BIS). Commodities, software and technology that do not fit into a specific ECCN are classified as "EAR 99" and, while they may be exported to most destinations, may still be controlled for export to certain sanctioned entities or a few prohibited destinations.

Empowered Official–The Empowered Official is defined in 22 CFR § 120.25. The Empowered Official has independent authority to: (i) inquire into any aspect of a proposed export or temporary import by the University, (ii) verify the legality of the transaction and the accuracy of the information to be submitted; and (iii) refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

Export – An Export occurs when a Controlled Physical Item or Controlled Information is transmitted outside the United States borders or when a controlled physical item or controlled information is transmitted to a Foreign Person in the United States. When a Controlled Physical Item or Controlled Information is transmitted to a Foreign Person in the United States, it is known as a deemed export. The term "Export" is broadly defined. It generally includes (1) actual shipment of any Controlled Physical Items; (2) the electronic or digital transmission of any Controlled Information; (3) any release or disclosure, including verbal disclosures and visual inspections, of any Controlled Information; or (4) actual use or application of Controlled Physical Items or Controlled Information on behalf of or for the benefit of a Foreign Entity or Person anywhere. Complete definitions of the term "Export" are contained in the federal regulations.

Foreign National – Any person other than a U.S. citizen, a lawful permanent resident of the United States (i.e., a "green card" holder), or a "protected individual" as defined in 8 U.S.C. §1324b (c) (1 & 2) (e.g., refugees or persons seeking asylum).

Foreign Person – For export control purposes, a Foreign Person includes any individual in the United States in nonimmigrant status (i.e., H-1B, H-3, L-1, J-1, F-1, B-1, and Practical Training) and individuals unlawfully in the United States.

A Foreign Person is also any branch of a foreign government or any foreign corporation or group that is not incorporated or organized to do business in the United States.

For export control purposes, a Foreign Person is not an individual who is a United States citizen, lawful permanent resident of the United States, a refugee, a person protected under political asylum, or someone granted temporary residency under amnesty or Special Agricultural Worker provisions.

International Visitors–International Visitors are Foreign Persons having a residence in a foreign country, which are not WTAMU employees or enrolled students and are coming to WTAMU on a temporary basis as a result of an invitation from a WTMU faculty member, researcher or administrator.

Knowledge – When referring to a participant in a transaction that is subject to the EAR, knowledge (the term may appear in the EAR as a variant, such as "know," "reason to know," or "reason to believe") of a fact or circumstance relating to the transaction includes not only positive knowledge that the fact or circumstance exists or is substantially certain to occur, but also an awareness that the existence or future occurrence of the fact or circumstance in question is more likely than not. Such awareness is inferred, inter alia, from evidence of the conscious disregard of facts and is also inferred from a person's willful avoidance of facts.

Manufacturing License Agreement – An agreement whereby a U.S. person grants a Foreign Person an authorization to manufacture defense articles abroad and which involves or contemplates: (a) the export of ITAR controlled technical data or defense articles; or (b) the use by the Foreign Person of ITAR controlled technical data or defense articles previously exported by a U.S. person. (ITAR § 120.21)

Material Transfer Agreements (MTAs) – A contract that governs the transfer and use of tangible research materials.

Non-disclosure Agreement (NDA) – A contract governing the use and disclosure of confidential and proprietary information.

Re-export – The transfer of articles or services to a new or different end-use, end-user, or destination.

Release – Technology or software is "Released" for export through: (i) visual inspection by Foreign Persons of U.S. origin equipment, facilities or documentation; (ii) oral or written exchanges of information in the U.S. or abroad; or (iii) the application to situations abroad of personal knowledge or technical experience acquired in the U.S..

Restricted Party Screening (RPS) – The process of determining whether a person or entity is included on the Specially Designated Nationals and Blocked Persons List.

Technology – Specific information necessary for the "development," "production," or "use" of a product. The information takes the form of "Technical Data" or "Technical Assistance."

Technical Assistance – May take forms such as instruction, skills training, working knowledge, and consulting services. Technical Assistance may involve the transfer of "Technical Data."

Technical Assistance Agreement – An agreement for the performance of ITAR-controlled defense services or the disclosure of ITAR-controlled technical data. (22 C.F.R. § 120.22)

Technology Control Plan (TCP) – A Technology Control Plan lays out the requirements for protecting export-controlled information and equipment for projects conducted at WTAMU.

Technical Data – Includes information "required for" the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. It 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, and read-only memories.

Trip Leader – A West Texas A&M faculty/staff/student leader(s) who conducts an international field trip or short program abroad and is accompanied by a group of students, either graduate and/or undergraduate.

Use – Operation, installation (including on-site installation), maintenance (including checking), repair, overhaul, and refurbishing.

Virtual Private Network (VPN) – A secure method of connecting to a private network at a remote location, using the internet or any unsecure public network to transport the network data packets privately, with encryption.

Appendix E – Purchasing Export Control Flow Chart