



TARLETON
STATE UNIVERSITY
Member of The Texas A&M University System

EXPORT CONTROL COMPLIANCE PROGRAM MANUAL

Revised November 11, 2020

TABLE OF CONTENTS

<u>Introduction and Commitment to Export Control Compliance</u>	4
<u>Responsibilities</u>	5
<u>Empowered Official</u>	5
<u>Compliance Program Administration</u>	5
<u>University Administrators</u>	5
<u>Departments/Units with Responsibility for Administering Program Components</u>	5
<u>Investigators</u>	6
<u>Faculty, Staff, and Students</u>	6
<u>Export Control Compliance Working Group</u>	7
<u>Relationship with other System Members</u>	7
<u>Decision-Making Assessment Tools</u>	7
<u>Identification of Export Control Concerns</u>	8
<u>Export Control Red Flags</u>	8
<u>Restricted Party Screening (RPS)</u>	8
<u>Jurisdiction Determination and Classification Review</u>	9
<u>International Traffic in Arms Regulations (ITAR) – United States Munitions List (USML)</u>	9
<u>Export Administration Regulations (EAR) – Commerce Control List (CCL)</u>	11
<u>Employment of Foreign Persons</u>	12
<u>Research</u>	13
<u>Contract Provisions of Concern</u>	13
<u>Specific U.S. Government Access and Dissemination Controls</u>	14
<u>Procedures Applicable to Research Agreements, Other Research-Related Agreements and Subcontracts</u>	15
<u>Resolving Export Control Concerns</u>	16
<u>Technology Control Plans (TCP)</u>	16
<u>Export Control License</u>	17
<u>International Visitors and Visiting Scholars</u>	17

<u>Required Notifications and Authorization to Host International Visitors or Visiting Scholars...</u>	17
<u>RPS of International Visitors</u>	18
<u>Access to Controlled Information or Controlled Physical Items</u>	18
<u>Admissions</u>	18
<u>Distance Education</u>	18
<u>International Activities</u>	19
<u>Study Abroad and Global Exchange (SAGE)</u>	19
<u>Screening Requirements</u>	20
<u>Purchasing and Financial Transactions</u>	20
<u>E-Commerce Accounting and Purchasing System Purchases</u>	20
<u>Procurement and Travel Card Purchases</u>	20
<u>Asset Management</u>	21
<u>Contract Administration</u>	21
<u>Technology Commercialization</u>	21
<u>Shipping</u>	21
<u>Travel</u>	22
<u>Gift Agreements</u>	23
<u>Recordkeeping</u>	23
<u>Training</u>	23
<u>Monitoring and Assessment</u>	23
<u>Possible Violation</u>	24
<u>Disciplinary Actions</u>	24
<u>Definitions</u>	25
<u>List of Abbreviations</u>	28

Introduction and Commitment to Export Control Compliance

This Export Control Compliance Program Manual (manual) is adopted by Tarleton State University (Tarleton or university) as a supplement to all United States export control laws and regulations, [The Texas A&M University System \(system\) Policy 15.02, Export Controls Program Management](#), and [Tarleton Rule 15.02.99.T1, Export Controls](#). The manual is designed as a guidance document to assist Tarleton faculty, staff, and students with export control compliance processes, procedures and requirements.

Tarleton is committed to ensuring compliance with System Policy 15.02, Tarleton Rule 15.02.99.T1, and all United States export control laws and regulations, including but not limited to those implemented by the Department of Commerce through the [Export Administration Regulations \(EAR\)](#), the Department of State through the [International Traffic in Arms Regulations \(ITAR\)](#), and the Department of Treasury through the [Officer of Foreign Assets Control \(OFAC\)](#).

Tarleton encourages and supports faculty, staff, students and collaborative relationships in the pursuit of securing resources for the advancement of the university's mission and goals. The university supports open research and the free interchange of information among scholars and the educational benefit to cultivate and invest in students as professionals that contribute to the advancement of the research, scholarship and economic enhancement of society.

The university also recognizes that the United States has enacted laws and regulations that restrict the shipment, transmission or transfer of certain items, software, technology and services from the United States to foreign countries, as well as "deemed exports" which are releases of controlled technology or source code to foreign persons located in the United States. These federal export control laws and regulations establish the conditions under which controlled information and controlled physical items can be transmitted to anyone outside the United States and to foreign persons in the United States. In addition, the export control laws and regulations restrict or prohibit the transaction of business with certain countries, persons and entities that have been sanctioned by federal agencies as a threat to important United States interests. Severe institutional and individual sanctions for violations of export control laws include the loss of research funding, loss of export privileges, as well as civil and criminal penalties including imprisonment. Although many university activities could be excluded from export control laws, some activities may be restricted. The application of export control laws involves a fact-specific analysis. While most exports do not require specific approval from the federal government, certain exports require a license and others are prohibited.

Questions related to export controls should be directed to the Department of University Compliance and Strategic Initiatives (CSI) as follows:

- By phone at 254-968-9415;
- By email at ExportControl@tarleton.edu; or
- In person at the CSI Office located in Room 106 of the Administration Annex I Building on the Stephenville campus.

Additional export control information and resources may be found on Tarleton's website at <https://www.tarleton.edu/compliance/compliance/export-controls.html>.

Responsibilities

Empowered Official (EO)

Tarleton's vice president for research or designee is herein appointed as the university's "empowered official" and delegated as the decision-making authority for the resolution of export control issues at Tarleton. The EO will coordinate with the System Research Security Office (RSO) and Office of General Counsel (OGC) prior to communicating with federal regulatory bodies and will collaborate with RSO, as needed, in the resolution of export control issues as needed.

Compliance Program Administration

The Office of University Compliance and Strategic Initiatives (CSI) is herein appointed as the responsible office and delegated authority for administration of Tarleton's export control compliance program.

CSI staff will represent the university on the system-wide export control affinity group and will collaborate and seek guidance from the EO and/or RSO, as needed.

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:

- (a) overseeing export control compliance in their areas of administrative responsibility;
- (b) supporting CSI in implementing the procedures set forth in this manual, and as otherwise deemed necessary by CSI to ensure export control compliance; and
- (c) completing TrainTraQ Training 2111212: *Export Controls and Embargo Basic Course* every two years and any other training recommended by CSI.

Academic deans, directors, department and unit heads have responsibility for overseeing export control compliance in their respective colleges, departments, units, centers, or institutes and supporting CSI in implementing procedures for export control compliance.

Vice presidents, directors and heads of other departments and units have responsibility for overseeing export control compliance in their units, where applicable, and supporting CSI in implementing procedures for export control compliance.

Departments/Units with Responsibility for Administering Components of Export Control Compliance

Tarleton departments/units, as determined by CSI, with responsibility for administering components of the university's export control compliance program must designate an individual(s) who will represent the department/unit and coordinate with CSI on export control compliance matters, including but not limited to, restricted party screening (RPS) and performing routine internal monitoring export control procedures and practices.

Designated liaisons must complete TrainTraQ Training 2111212: *Export Controls and Embargo Basic Course* every two years and any other training recommended by CSI.

Designated liaisons will serve on Tarleton's Export Control Compliance Working Group and should attend

applicable meetings.

Applicable departments/units, their administrators, and designated liaison(s) are responsible for developing and maintaining written internal departmental procedures for administering their component of export control compliance.

Investigators

Investigators (includes principal investigators, co-principal investigators and co-investigators), with the assistance of CSI, the Office of Research and Innovation (ORI) and other applicable departments, units and individuals, are responsible for full compliance with all federal and university export control requirements in the conduct of their research.

Violation of export control laws can directly affect investigators through potential fines, loss of research funding, personal criminal liability, and/or disciplinary action, up to and including dismissal.

Each investigator must:

- understand their individual export control obligations and participate in regular trainings to be able to identify export control concerns;
- be aware of the export control red flags outlined in the university's Export Control Compliance Program Manual and note such information on any internal compliance or assurance forms;
- determine, prior to initiation of research, whether any information or technology involved in their research is subject to export control laws or regulations;
- review their research periodically to ensure continuing compliance with export control laws and regulations;
- brief students and other researchers involved in the project of their export control obligations, if undertaking an export controlled project;
- understand that any information agreement or understandings entered into with a sponsor may negate the fundamental research exclusion or other key exclusions and impose export control obligations on the investigator;
- understand that any communication of technical data to a foreign person or to anyone outside the United States could be considered a deemed export or an export and, therefore, subjected to export regulations;
- contact CSI with export control questions or concerns; and
- report possible or actual violations of United States export control laws or regulations as outlined in section 2.6.4 of this manual.

Faculty, Staff and Students

All faculty, staff and students must be aware of, are responsible for the export control implications of their work, and must ensure that their activities conform to all export control laws, regulations, policies, rules and guidelines.

All university employees must complete TrainTraq Training 2111212: *Export Controls and Embargo Basic Course* every two years. Depending upon the nature of their activities and/or job functions, university personnel may be required to complete additional TrainTraq training courses and/or participate in formal training as determined by CSI and/or the employee's supervisor.

CSI will provide assistance to faculty, staff and students in assessing the applicability of export control regulations; however, primary responsibility for compliance rests with the individuals involved in the export, including principal investigators and others in supervisory positions.

Each university employee has the responsibility to report possible violations of United States export control laws or regulations. Suspected violations must be immediately reported by one of the following methods:

- CSI can be contacted by phone at (254) 968-9415, by email at ExportControl@tarleton.edu or in person in their office located on the Stephenville campus in Room 106 of the Administration Annex I Building;
- Through Tarleton's Compliance Help and Reporting confidential reporting tool on the Compliance webpage at: <https://www.tarleton.edu/safety/compliance/index.html>; or
- Through the EthicsPoint website at: <https://secure.ethicspoint.com/domain/media/en/gui/19681/index.html>.

All university faculty, staff, and students must adhere to all United States export control laws and regulations, system policies and regulations, university rules and guidelines and training requirements.

Export Control Compliance Working Group (working group)

Tarleton's working group will be chaired by CSI staff and consist mainly of designated department liaisons, as defined in 2.4 of this rule, who have been designated the responsibility for administering components of the university's export compliance program. The working group may also include subject matter experts, campus partners and administrators, and the EO, as needed. Responsibilities include, but are not limited to, assessment of the university's export control compliance program and department compliance components, departmental responsibilities and internal procedures, collaboration and process improvement. The working group will meet at minimum on a bi-annual basis or more frequently as needed.

Relationship with Other System Members

Other system members maintain their own export control compliance programs to ensure compliance with export control laws and regulations. To the extent there are overlapping export control compliance obligations, such as when university faculty, research, facilities or equipment are concerned, the applicable system members should coordinate with CSI.

Decision-Making Assessment Tools

CSI has developed an [online decision-making assessment tool](#) to assist individuals in analyzing potential export control issues and required steps to assist in ensuring export control compliance at Tarleton. In addition, risk specific decision-making resources independent of this assessment tool have also been developed to assist the Tarleton community in ensuring export control compliance. These resources may be located on [Tarleton's export control webpage](#) and discussed in applicable sections within this manual.

Identification of Export Control Concerns

Export Control Red Flags

Indicators that an export control review should be conducted to mitigate the risk of violations includes, but is not limited to:

- The results of research conducted at Tarleton or by Tarleton employees are intended for military or space purposes or for other restricted end uses or users;
- Foreign persons will have access to controlled information or controlled physical items on campus;
- Software including encryption features will be developed or purchased;
- Tarleton 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, tablets, portable devices, or any electronic device capable of storing or containing controlled information;
- A proposed activity or transaction will involve embargoed countries or entities, individuals/entities located in embargoed countries, or who are on prohibited or restricted end-user lists, as determined by restricted party screening (RPS);
- The sponsor requires pre-approval rights over publications or the participation of foreign persons;
- The project requires shipping, hand-carrying or electronic transfer of items outside the United States including, but not limited to, equipment, chemicals, data, biological materials, etc.;
- The agreement contains a controlled unclassified information (CUI) clause. (e.g. DFARS 252.204-7012; or
- Other red flag indicators: The Department of Commerce, Bureau of Industry and Security has posted a checklist of *Things to Look for in Export Transactions* located on their website at <http://www.bis.doc.gov/index.php/enforcement/oeec/compliance/23-compliance-a-training/51-red-flag-indicators>.

Restricted Party Screening (RPS)

The U.S. Department of Commerce, the U.S. Department of State, and the U.S. Department of Treasury, along with various other government agencies, maintain lists of prohibited and restricted end-users (restricted party lists). In order to ensure that Tarleton 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, Tarleton must screen individuals and entities as provided in this manual. Restricted party screening (RPS) is the process of determining whether a person or entity is included on a restricted party list.

Tarleton has licensed export control compliance software that permits authorized users to screen restricted party lists electronically. The export control compliance software performs RPS against relevant U.S. Government lists, including, but not limited to: Department of Treasury Office of Foreign Assets Control (OFAC) Specially Designed Nationals List, Department of Commerce BIS Entry List and Unverified List, Department of State Arms Export Control Act Debarred Parties, Department of State Designated Terrorist Organizations, and Department of State Nonproliferation Orders.

Authorized Users

Tarleton designated liaisons with a business need to access and use the software must first complete TrainTraq Training 2111212: *Export Controls and Embargo Basic Course* before submitting a [Request to Activate/Deactivate Access to Export Control Compliance Software form](#) to CSI. No access or use will be authorized without CSI approval. CSI will perform RPS screening of the individual using the export control compliance software and document on the request the requestor's completion date of the required training course before submitting the approved request form, along with RPS documentation, to the TAMU Export Control Office (TECO).

CSI must notifying and submit a [Request to Activate/Deactivate Access to Export Control Compliance Software form](#) to TECO if any authorized employee's status changes so that access can be deactivated. Authorized users are limited to United States citizens and legal permanent residents who are full-time employees of the system or a system member. Authorized users will be limited to full time employees with business need only. CSI may limit the number of authorized users, as it deems appropriate.

Responsibilities

Designated liaisons, authorized to conduct RPS, should conduct RPS in accordance with their department's/units internal procedures. If there is a possible match of the party being screened with a party on a restricted party list (a "hit"), a secondary review should be conducted by using additional detailed information. If the hit cannot be dismissed on secondary review, the matter should be referred to CSI along with the criteria used to determine the possible match for secondary screening. Upon further investigation, CSI will make and notify the designated liaison of the determination. CSI is responsible for maintaining records of its determinations. The departments/units of designated liaisons are responsible for maintaining records of determinations that are not forwarded to CSI, as provided in the Recordkeeping section of this manual. If concerns or issues cannot be resolved by the secondary screening, the matter may be referred to the EO and/or RSO for guidance and resolution, when appropriate.

Annual Review of Authorized Users/Screeners

On an annual basis, CSI will review the list of authorized users to confirm that the individuals listed are still appropriately authorized for that specific department/unit. Authorizations will be limited to those with business need only. CSI may limit the number of authorized users as it deems appropriate.

Jurisdiction Determination and Classification Review

The U.S. Department of Commerce, and the U.S. Department of State, along with various other government agencies control what technology, items, goods, services, etc. (Technology) may be exported outside of U.S. territory and to Foreign Persons in the United States. If an item is export controlled, prior authorization from one of the government agencies (e.g., Department of Commerce or State) may be required to transfer the item internationally; and/or depending on the type of item (EAR or ITAR) and the circumstances in which it is being accessed and used, Foreign Person access to (or use of) the item may be restricted unless specifically authorized by the governing agency.

International Traffic in Arms Regulations (ITAR) – United States Munitions List (USML)

USML Categories - The Department of State regulates exports of Defense Articles and Defense Services via the International Traffic in Arms Regulations (ITAR) which can be found at 22 CFR 120-129 (https://www.pmdtc.state.gov/ddtc_public). The ITAR includes a list of articles, services and related Technical Data designated as Defense Articles and Services regulated by the federal government known as the United States Munitions List (USML) (See 22 CFR 121.1). Categories include:

- Firearms, Close Assault Weapons and Combat Shotguns
- Guns and Armament
- Ammunition/Ordinance
- Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
- Explosives, Energetic Materials, Propellants, Incendiary Agents and Their Constituents
- Surface Vessels of War and Special Naval Equipment
- Ground Vehicles
- Aircraft and Related Articles
- Military Training Equipment and Training
- Personal Protective Equipment
- Military Electronics
- Fire Control, Laser, Imaging and Guidance Equipment
- Materials and Miscellaneous Articles
- Toxicological Agents, Including Chemical Agents, Biological Agents and Associated Equipment
- Spacecraft and Related Articles
- Nuclear Weapons Related Articles
- Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated
- Directed Energy Weapons
- Gas Turbine Engines and Associated Equipment
- Submersible Vessels and Related Articles
- Articles, Technical Data and Defense Services Not Otherwise Enumerated

ITAR defense items are broadly defined to include any item or equipment, related Technology, software or data that is built, compiled, specially designed, or modified to military or defense specifications. This can include precision electronics, components and instruments used during the course of fundamental research. The fact that TAMU can procure such an item commercially does not necessarily mean that the item is not a Defense Article. In some cases, a vendor or provider of such item may label it ITAR, which flags it as an export controlled defense item.

It is important to keep in mind that ITAR restrictions apply even in the context of open laboratory, fundamental research projects where no citizenship or publication restrictions have been accepted. Therefore, determining whether or not an item is ITAR controlled prior to incorporation into research inventory or utilized by an Investigator or research team is essential. The fact that the item can be purchased commercially does not remove its controlled status. Buyers, licensees or other types of recipients of ITAR items remain responsible for managing the applicable Foreign Person restrictions. To better understand what is regulated under ITAR, it is important to read the regulations in the context of the definitions for Defense Article, Defense Service, and Technical Data. Below are the definitions as well as a link to the State Department's website which may be of assistance in understanding and applying the federal regulations, (https://www.pmddtc.state.gov/ddtc_public).

- Defense Articles (22 CFR 120.6) are broadly defined to include any item or equipment, related Technology, or Technical Data that is built, compiled, designed, or modified to military specifications. This includes, for example, military-grade electronics and components of instruments even if they are used during the course of fundamental research. It also includes items or Technical Data with significant military or intelligence applicability. The fact that the item is commercially available does not necessarily mean the item is not a "Defense Article." Defense Articles include: hardware, software, Technical Data recorded or stored in any physical form, models, mockups or other items

that reveal Technical Data. It also includes forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as Defense Articles. It does not include basic marketing information on function or purpose or general system descriptions.

- Defense Service (22 CFR 120.9) is defined as (1) furnishing of assistance (including training) to Foreign Persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of Defense Articles; (2) furnishing to Foreign Persons of any controlled Technical Data, whether in the United States or abroad; or (3) military training of foreign units and forces, regular and irregular, including formal or informal instruction of Foreign Persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.
- Technical Data (22 CFR 120.10) is defined as information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of Defense Articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation; information covered by a secrecy order; and software directly related to a Defense Article; classified information relating to Defense Articles and Defense Services on the USML 12 and 600-series items controlled by the Commerce Control List; and software directly related to Defense Articles.

Export Administration Regulations (EAR) – Commerce Control List (CCL)

The Department of Commerce regulates exports of Dual-Use items and Technology via the Export Administration Regulations which can be found at 15 CFR Parts 730-774

(<https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>). The EAR includes a list of items subject to regulation known as the Commerce Control List (CCL). The CCL can be found at <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>. Categories and Product Groups include:

Categories:

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

Product Groups:

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

- D - Software
- E - Technology

Using the above categories and product groups, an Export Control Classification Number (ECCN) can be determined. The ECCN is a 5 character alpha numeric code. The first character is a number that describes the category of the item. The second character is a letter which indicates the product group. The last 3 numerical digits are used for numerical ordering of the item. If an item falls under U.S. Department of Commerce jurisdiction and is not listed on the CCL, it is designated as EAR99. EAR99 items generally consist of low technology consumer goods and do not require a license in many situations. However, if the item will be exported to an embargoed country, to an End-User of concern, or in support of a prohibited End-Use, a license may be required. The federal government's recent Export reform initiative has resulted in some changes to the USML and CCL. Some Defense Articles that were once listed on the USML have now moved to the CCL creating two new series of ECCNs: 500 for Spacecraft and 600 for 13 Commerce Munitions. Items that moved from the USML to the CCL have generally included some less important parts, components, accessories and attachments used in or with Defense Articles. The federal government uses a "catch" and "release" process to determine if items stay on the USML or are released onto the CCL. If the item is not on the revised USML, or within one of the "specially designed" catch-all, the item is "released" to the CCL and controlled under the specifically enumerated ECCN. For BIS FAQs and policy guidance, see <https://www.bis.doc.gov/index.php/policy-guidance/faqs>; and <https://www.bis.doc.gov/index.php/policy-guidance>.

Dual-Use items are broadly defined as any item (equipment, instrument, related technology, material, software or data) that is civilian by design and intended application, but could, by virtue of its specifications and performance, be used for a defense purpose. Dual-Use items can include research instruments and related software, materials, or data used in fundamental research. The fact that TAMU can procure such items commercially does not mean that they are not export controlled. In some cases, a vendor or provider of an item may label it as EAR-controlled, which flags it as a Dual-Use export controlled item.

For Dual-Use items, it is important to identify situations where Dual-Use Controlled Technology that is not otherwise the subject of fundamental research and eligible for publication is potentially shared or utilized. Below are several examples of Technology sharing, which may trigger an export control issue:

- Utilizing vendor-proprietary repair or maintenance manuals, or software configuration programs, provided by a vendor (or third party);
- Training research personnel to perform all of the following functions with respect to a specialized research instrument: install, maintain, repair, refurbish and overhaul (or any combination of these items) that imparts the inherent proprietary design and controlled functionality of a Dual-Use controlled item (again, presumes having a vendor's proprietary installation/repair manual or software configuration program); and
- Developing or modifying a Dual-Use instrument (typically a co-development arrangement with a vendor or manufacturer) that likewise exposes the underlying controlled design. Development may include all stages of work prior to serial production, such as design research, analysis, "proof of concept," assembly and testing of prototypes, pilot production schemes, configuration, or integration design.

Employment of Foreign Persons

It is important for hiring departments/units to be aware that the ability to hire nonimmigrant foreign persons

for certain positions may be restricted or prohibited by export control laws. For example, nonimmigrant foreign persons may be restricted or prohibited from performing employment responsibilities relating to certain positions to the extent the work will involve access to controlled information or items.

Supervisors proposing to hire foreign nationals should carefully consider whether or not the proposed employment will involve access to controlled information or items before extending offers of employment. When a foreign national is proposed for employment at Tarleton, the hiring supervisor or principal investigator, in consultation with Employee Services (ES), must:

- Complete TrainTraq Training 2111212: *Export Controls and Embargo Basic Course*, if they have not already done so within the past year; and
- Complete and submit a [Checklist for Export Control Issues When Hiring Foreign Nationals](#) to Employee Services (ES).

ES will conduct RPS in accordance with section 4.2.2 of this manual. Export control concerns and issues related to the hiring of foreign nationals will be referred to CSI for secondary screening. If concerns or issues cannot be resolved by the secondary screening, the matter may be referred to the EO and/or RSO for guidance and resolution, when appropriate.

Research

Most data and information involved in university research is excluded from export control regulation under the ITAR or EAR based on “Published” technology and software/public domain exclusion (PDE) and the fundamental research exclusion (FRE). 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, investigators 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 also important to remember that the restrictions enforced by OFAC are not affected by the ITAR, EAR, or FRE. OFAC restrictions and prohibitions generally arise in connection with interactions involving certain individuals, entities and countries most notably in interactions with embargoed countries and individuals/entities from embargoed countries. A list of current embargoed/sanctioned countries may be found on the Bureau and Security (BIS) webpage at: <https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations>.

Contract Provisions of Concern

Certain research agreement provisions may negate the FRE and require seeking a license, undertaking monitoring or other activities. These provisions of concern are identified on the Issues are identified on the [Tarleton Export Control Decision-Making Tree for Administration of Contract Provisions of Concern](#) and are summarized below.

If any of the following provisions are present (and cannot be negotiated away) in a research agreement or subcontract, or other non-sponsored research agreement (e.g., a Material Transfer Agreement (MTA), or Non-Disclosure Agreement (NDA) related to research), CSI, and the EO when necessary, should be consulted for guidance prior to execution of the agreement.

- Sponsor maintains the right to restrict or approve publication or release of research results (other than Tarleton’s standard customary brief delay to protect a sponsor’s confidential information or to

- preserve the patentability of an invention);
- Research data and/or other research results will be owned by the sponsor (e.g., as sponsor's proprietary or trade secret information);
- Statements that export control restrictions will apply to the research;
- 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;
- Restrictions on, or prohibitions against, the participation of research personnel based on citizenship or national origin;
- Statements that the sponsor anticipates providing export-controlled items or information for use in connection with the research;
- Equipment or encrypted software is required to be delivered as part of the project;
- The research project will involve the use of export-controlled items or technical information obtained from a third party;
- There is a Controlled Unclassified Information (CUI) clause (e.g., DFARS 252.204-7012); or
- The research will take place outside the United States (e.g., attending conferences, shipping items internationally, and international collaborations).

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 is 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 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 27.405-1 for more information.

DFARS 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& (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.

DFARS 252.225-7048 (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 investigator 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. The 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 17 clause is commonly found in contracts involving controlled technology and sponsored by military agencies. Investigators may need 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 the investigator is doing basic research and the sponsor will take those results and work on the controlled technology at another location, the clause may be able to be deleted.

ARL 52.005-4401 (Release of Information)

Includes reference to “non-releasable, unclassified information” and a requirement to “confer and consult” prior to release of information. It is unclear what the review entails. Therefore, 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 person to work on the project or allowing foreign persons access to the work, equipment, or technical data generated by the project. CSI, and the EO when appropriate, needs to be notified if this clause is included in the contract.

DFARS 252.204-7012 (Controlled Unclassified Information)

Requires 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://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm), to protect controlled unclassified information (CUI) on non-Federal information systems. For full text see <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>.

Procedures Applicable to Research Agreements, Other Research-Related Agreements and Subcontracts

In the case of sponsored research agreements administered through SRS, processes and procedures have

been established.

For other sponsored research related agreements and non-sponsored research agreements (e.g., Material Transfer Agreements, Non-Disclosure Agreements, Data Transfer Agreements, etc.) administered through ORI, processes and procedures have been established.

Resolving Export Control Concerns

When a potential export control concern is identified, CSI will work with the parties involved, the EO and RSO, when appropriate, to determine what course of action should be taken to address the concern. In many cases, no license or other authorization may be necessary. In each case, RSO will assist CSI and EO in determining 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 applicable;
- (c) *Technology Control Plan* (TCP), or other requirements for the conduct of the research, will be necessary to prevent an unauthorized deemed export of the technology from occurring;
- (d) Additional actions are required as determined by CSI, RSO and/or the EO are necessary to ensure compliance; or
- (e) A possible violation of United States export control laws or regulations that will warrant further investigation or actions in accordance with investigation/or actions outlined in Tarleton's rule.

CSI or the EO, when appropriate, will notify the parties involved of the export control determinations. CSI will maintain records of its determinations on a project basis, as provided in the Recordkeeping section of this manual.

[Technology Control Plans \(TCP\)](#)

If CSI determines a project, facility, or item is export-controlled, CSI will work with the PI and/or facility managers, as appropriate, to develop and implement a TCP to secure the controlled technology from access by unauthorized foreign persons. A TCP will typically include:

- A commitment to export controls compliance;
- Identification of the relevant export control categories and controlled technologies;
- Identification of the project's sponsors;
- Identification and nationality of each individual participating in the project;
- Appropriate physical and informational security measures;
- Personnel screening measures and training; and
- Appropriate security measures for the duration of the project for and following project termination.

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

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

individuals cannot observe or access controlled items or information.

- **Marking.** Export-controlled items or information must be clearly identified and marked as export-controlled.
- **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.
- **Locked Storage.** Tangible items such as equipment, associated operating manuals, and schematic diagrams should be stored in rooms with key-controlled access. Soft and hardcopy data, lab notebooks, reports, and other research materials should be stored in locked cabinets.
- **Electronic Security.** Project computers, networks, and electronic transmissions should be secured and monitored through User IDs, password controls, 128-bit Secure Sockets Layer encryption, or other federally approved encryption technology. Database access should be managed via a virtual private network (VPN).
- **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.

CSI will perform and document an annual site visit for all active TCPs.

Export Control License

If an ITAR, EAR, OFAC or other license, Technical Assistance Agreement, Manufacturing License Agreement, Registration, or other authorization is needed, CSI will consult with the investigator and other appropriate parties to gather all the information needed to submit the appropriate documentation to seek a license through RSO. CSI will inform the EO, or designee, of the details of the export control concern and make a recommendation that a license or other authorization should be obtained. CSI, or the EO when appropriate, will request the license or other authorization from the cognizant agency with assistance from RSO and OGC, as appropriate.

International Visitors and Visiting Scholars

Tarleton personnel, departments or units intending to invite or host any international visitors or visiting scholars (host) should be aware that there might be restrictions or prohibitions associated with such visits. For example, (i) the proposed visitor is from an embargoed country, (ii) the proposed visitor or affiliated institution appears on a restricted party list, or (iii) the proposed activities require an export license. Hosts should carefully consider possible export control implications and obligations associated with a proposed visit and should consult with CSI before making any commitment to host an international visitor or visiting scholar in accordance with the process outline herein.

Required Notifications and Authorization to Host International Visitors or Visiting Scholars

Before extending a formal invitation or agreement/commitment, Tarleton personnel, departments or units intending to invite or host international visitors or visiting scholars are required to complete and submit to CSI an [International Visitor/Visiting Scholar Export Control Compliance form](#) for export control compliance screening and approval. Additional information may be requested by CSI to complete the compliance review and screening process.

If screening results do not raise any concerns or restrictions, CSI will provide written notification to the host of export control compliance approval. If screening results raise concerns and/or restrictions, CSI may refer the matter to the EO and/or RSO for guidance and/or assistance with resolution, when appropriate. The host may be contacted in an attempt to resolve the concerns and/or restrictions, when possible. If resolution is not possible, the EO will deny the visit and written notification of the denied request will be provided to the host. If the concerns and/or restrictions are resolved, the host will be notified in writing of approval and any applicable restrictions for the visit.

In addition, written approval for any research activities for such visits must be obtained from ORI in advance of an official invitation or agreement/commitment to host. When appropriate, a copy of the approval will be sent to the Center for Education Excellence (CEE) to initiate the any necessary related immigration processes.

In the event it is anticipated that the nature, purpose or duration of a visit will change, the host must provide written notification to CEE, with a copy to CSI, to obtain approval and to update of any necessary documentation prior to the effective date of the change.

RPS of International Visitors

RPS is required for all international visitors or visiting scholars, and includes, but is not limited to, RPS screening the international visitor or visiting scholar, affiliated institution(s) and/or sponsoring entity. RPS is required in advance of written or verbal invitation or agreement/commitment to host any international visitor or visiting scholar.

Access to Controlled Information or Controlled Physical Items

No international visitor or visiting scholar may have access (whether verbal, written, electronic, and/or visual) to controlled information or controlled physical items expressly permitted via an approved Technology Control Plan (TCP), an export control license has been obtained or authorization in writing by CSI or the EO. It is the responsibility of the university personnel and department or unit hosting the visitor to ensure compliance with export control regulations and to promptly disclosed and reported to CSI.

Admissions

The Department of Admissions performs authentication of student admissions materials and required identification and immigration documentation. A primary Restricted Party Screening (RPS) is performed by the Department of Admissions for all foreign nationals seeking admission to the university with a secondary screening by CSI, as needed. CSI will seek guidance from the EO and/or RSO as needed for resolution of concerns and for decision-making regarding admission approval. Foreign persons will not be admitted to the university until they have been cleared through the export control screening process.

Distance Education

Distance education (DE) at Tarleton refers to credit bearing, transcribed courses only offered to enrolled and registered students, where the course delivery occurs in a setting where the students and faculty member of record are not in the same place at the same time or where the instruction for the course occurs at an approved off-campus educational site. This instruction can be in the form of 100 percent online, face-to-face offsite, or some hybrid combination of face-to-face and online. Due to the element of distance in this

education delivery method, some export control concerns may arise.

It is the responsibility of the department offering the course and the faculty instructor of record to ensure export control requirements are reviewed and any concerns addressed with CSI. Under the guidance of the Provost's Office and as part of the standard new course approval process, the instructor of record for each DE course must complete a [Distance Education Courses Checklist](#) (DE checklist) and review [The Texas A&M University System Export Control Distance Education Decision Tree](#) (DE decision tree) to determine compliance with export control laws and regulations. If the DE checklist or decision tree indicate the need for export review, the DE checklist must be forwarded to CSI for further review and CSI approval will be required prior to course approval. If through screening CSI determines that export control concerns exist, CSI will work with the instructor and RSO and/or the EO, as needed, to resolve the concerns.

Additionally, confirming the identification of students enrolled in distance education is necessary and standard operating procedure for all courses, whether the student is foreign or domestic. Regardless of course delivery method, a primary Restricted Party Screening (RPS) is performed by the Department of Admissions for all foreign nationals seeking admission to the university with a secondary screening by CSI, as needed. Beginning with the student admission process, student identification is authenticated by the review of student admissions application materials, further identification provided during financial aid and housing application, issuance of a Universal Identification Number (UIN) and unique password. The authenticated UIN and password are used to gain access to a variety of student resources including student registration and information portal, as well as the e-learning resources utilized in delivery of distance education.

Furthermore, a listing of students enrolled in distance education courses from a foreign location is produced by the Department of Institutional Analytics, Effectiveness and Accreditation and provided to CSI on a daily basis for review and screening.

If any student is identified as ineligible for participation in a course offered via distance education, the Office of the Registrar, in concert with the department facilitating the desired course, will remove the student from the course registration and block access to the course e-learning resources.

International Activities

Academic Affairs, the Center for Education Excellence (CEE), the Office of Diversity, Inclusion, and International Programs (DIIP), or other office(s) as appropriate, in coordination with CSI, are responsible for developing and implementing procedures to screen international programs, centers, and activities for compliance with export control laws and regulations. In the case of university activities conducted outside the United States, it is the responsibility of the university activity organizer and/or international programs or other applicable official(s) to seek and obtain appropriate export control approvals from CSI for activities including, but not limited to, the following: execution of agreements performable outside the United States; execution of agreements with export control requirements; execution of agreements and binding commitments with foreign entities; education abroad courses and activities; exchange students, and making payments to foreign person vendors.

Study Abroad and Global Exchange (SAGE)

SAGE programs are administered by CEE. CEE will ensure SAGE activity organizers and leaders are aware of and required to abide by applicable export control laws, system policies and regulations, and university rules and procedures. Program and activity leaders are provided information and materials to alert them of export control compliance responsibilities and requirements and to assist students who

participate in the program or activity.

Screening Requirements

All requests for foreign travel must be submitted in accordance with the university's Foreign Travel Procedures and will be routed through CSI for export control compliance screening and approval.

International Program or Activity Students Subject to RPS

All foreign persons, who are not enrolled as a student in a credit-bearing program at Tarleton, who are attending courses and/or receiving instruction at an international center or are participating in a Tarleton non-credit bearing international program, activity, global exchange, or field trip abroad will undergo RPS prior to participation.

International Program or Activity Faculty and Scholars Subject to RPS

All foreign persons teaching, conducting research, or presenting workshops, symposia, or other academic presentations at an international center and/or during a Tarleton-sponsored international program or activity who are not employed by Tarleton will undergo RPS prior to participation in any university-sponsored international program or activity.

Screening Procedures

It is the responsibility of the program and/or activity organizer or leader to ensure that CSI is provided required information for applicable foreign persons for screening purposes as soon as reasonably possible once identified. The identified foreign persons will not allowed to participate in programs or activities until screened and approved in writing by CSI.

Purchasing and Financial Transactions

Requisitioners, purchasers and reviewers should review the [Export Control Purchasing Guidance document](#) to determine if items purchased or to be purchased may be subject to export control regulations. If review of the guidance document indicates an item(s) may be subject to export control regulations, the individual should contact CSI for further review and guidance before making the purchase.

E-Commerce Accounting and Purchasing System Purchases

RPS is conducted by Texas A&M University Financial Management Operations for all vendors at the time vendors are established through the vendor setup process in Tarleton's e-commerce accounting and purchasing system (e-commerce system). During the purchasing process, commodity codes associated with export-controlled items are identified and flagged by the e-commerce system so that requisitions are routed to CSI for screening, approval, determination of U.S. Export Control Classification, and any further actions (such as export control license, Technology Control Plan, etc.) deemed necessary by CSI to ensure export control compliance. CSI will provide written notification to the requisitioner and/or department head that the item(s) purchased may be subject to export control regulations, requirements, and any actions necessary to ensure compliance.

Procurement and Travel Card Purchases

Individuals making purchases with university issued procurement or travel cards will be responsible for ensuring

their purchases comply with export control laws and regulations. The office of Business Services reviews all procurement and travel card expenses post-purchase and will route to CSI if any suspected export-controlled items for post-purchase review, acknowledgement, and follow-up actions deemed necessary by CSI to ensure export control compliance.

Asset Management

Items identified through purchasing review and within Tarleton's inventory as export controlled are documented by CSI, Technology Control Plans (TCP) are developed and tracked as deemed necessary. CSI will perform and document an annual site visit for all active TCPs.

Contract Administration

Per the President's Delegation of Authority, identified types of contracts will be routed to CSI for export control compliance review, screening, and approval before execution by the delegated authority. Any contract or agreement with a foreign entity or person will be routed to CSI for export control compliance review, screening, and approval before execution by the delegated authority. Any contract or agreement including export control language or clauses will be routed to CSI for export control compliance review, screening, and approval before execution by the delegated authority.

Technology Commercialization

CSI will refer any activity that may result in proprietary and/or patentable products and potentially subject to export control restrictions to the TAMUS – Office of Technology Commercialization for review and handling as appropriate.

Shipping

Items shipped internationally for university business should be shipped through Tarleton's Central Receiving or Tarleton's Post Office to ensure compliance with export control laws and regulations. CSI must be notified and screen international shipments for university business prior to shipping through an off-campus shipping carrier, agent or agency.

Before shipping items internationally for university business through Central Receiving, CSI should be contacted by email at ExportControl@tarleton.edu or by phone at (254)968-9415 to perform RPS. The individual shipping the items must complete an [International Shipping Form](#), attach the RPS cleared results, and provide the documentation to Central Receiving with the shipment. Following shipment, Central Receiving provides shipping documentation by email to ExportControl@tarleton.edu.

The Tarleton Post Office will follow [United States Postal Service Guidelines](#) for international shipping.

It is the responsibility of Tarleton employees or students who are shipping items outside the United States (including hand-carrying items such as research equipment, materials, data, or biological materials) to comply with export control laws and regulations. Any transfer of project information, items, equipment, materials, or technology out of the U.S. by any method may be subject to export control restrictions and may require an export license or be prohibited depending on the item, destination, recipient, and end-use. Even if an item is cleared through customs, it may still require an export control license. The simple act of sending a package to a foreign collaborator can result in a violation of export control laws and regulations.

Additionally, Central Receiving and/or CSI must first clear shipping to countries subject to an embargo. Departmental personnel or students who are responsible for shipping packages out of the country should obtain a list of contents before shipping and contact CSI with any questions. Shipping controlled 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 Tarleton as well. One should not ship any item internationally without taking the time to find out if a license is required. Mislabeling the package or misrepresenting the classification of the item is illegal. Violations may result in civil penalties, and deliberate violations may result in criminal prosecution. Under-invoicing or undervaluing an exported item is also against the law. Reporting an incorrect export value on a Shipper's Export Declaration is a violation of export regulations. Shipment of items controlled under the ITAR or EAR should be clearly marked as controlled with the appropriate regulatory control cited. Any licensed export, regardless of dollar value, as well as exports with a dollar value greater than \$2,500, regardless of export control status, must be entered into the Department of Census Automated Export Control System (AES) prior to the export of the item or information.

Travel

All requests for foreign travel must be submitted in accordance with the university's [Foreign Travel Procedures](#) and will be routed through CSI for export control compliance screening and approval. Upon receipt up the request for foreign travel, CSI will perform RPS and provide additional information to the traveler along with a request for:

- A completed *International Travel Export Control Questionnaire* for further review and screening by CSI; and
- A completed [Temporary Imports, Exports, and Reexports \(TMP\) Certification](#) emailed to both CSI and Information Technology Security, if the traveler intends to travel with a Tarleton loaner laptop or any university owned portable electronic device.

Tarleton employees and students traveling on Tarleton business or traveling with Tarleton property are responsible for complying with export control laws and regulations when traveling outside the U.S. 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. The traveler or the traveler's supervisor should contact CSI with any potential export control concerns or questions.

When planning a trip abroad, travelers should review export control regulations and embargoes. Individuals should ensure that any information that will be discussed or any items that will be taken are not controlled, or, if controlled, that appropriate licenses are in place. Not only could Tarleton be held liable, but individuals may also be held liable for improperly transferring controlled information or controlled physical items.

If a member's of Tarleton's faculty or staff must travel with a portable electronic device (device), it is recommended that a "clean" university-owned loaner device be requested from Information Technology Services (ITS) in lieu of traveling with a university assigned or personal device. To do so, travelers will need to submit an ITS Computer Help Desk ticket on the ITS website to request a clean loaner device (e.g. laptop, MacBook, tablet, etc.) for travel. ITS will need at least one week to prepare a clean loaner device for your use during the subject travel. Using a clean loaner device greatly reduces the risk of loss, theft, or inadvertent disclosure of export-controlled or protected information. If you choose to take a device other than a clean university loaner device deployed to you by ITS, you must notify ITS Security at itsecurity@tarleton.edu at least ten (10) working days in advance of your departure for the subject travel so that they are aware and can provide you with additional resources and best practices. If devices are taken abroad that contain encrypted software,

a government license or other government approval for export may be required when traveling to certain countries.

Researchers frequently need to take other Tarleton equipment temporarily outside of the United States 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. In such instances, travelers should contact CSI for guidance and determination if an export license or other government approval is required prior to taking the equipment out of the country. It is important to note that activities involving teaching or training foreign persons on how to use equipment may require a license.

Gift Agreements

The Office of Advancement Services will perform an initial review all gifts for red flags and those from foreign entities. CSI will be notified if any gifts are received with red flags or from foreign entities and will be documented on an *Export Control Gifts Worksheet* with RPS performed. In addition, Advancement Services will send a weekly report of all Tarleton gifts to CSI for further review and actions, as needed.

Recordkeeping

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

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

Records will be maintained by CSI or as otherwise designated in this manual, and accessible for audit/assessment purposes. Those conducting RPS are expected to maintain documentation of RPS results including documentation indicating the methodology for determinations.

Training

CSI, in coordination with RSO, OGC and/or the EO as needed, will develop and implement an appropriate university training program.

All university employees must complete TrainTraq Training 2111212: *Export Controls and Embargo Basic Course* every two years. Depending upon the nature of their activities and/or job functions, university personnel may be required to complete additional TrainTraq training courses and/or participate in formal training as determined by CSI and/or the employee's supervisor.

Monitoring and Assessment

In order to maintain Tarleton's export compliance program and ensure consistent adherence to U.S. export control laws and regulations, CSI will conduct regular and as needed internal reviews and monitoring of all

aspects of the university's export control program including but not limited to RPS, TCPs, and projects requiring documentation for RPS. The purpose of the reviews is:

- to identify possible violations; and
- to identify deficiencies in training, procedures, etc., that can be rectified.

Findings will be reported to the university compliance officer, EO and/or president as appropriate.

Annually, CSI will conduct a risk assessment of the university's export control compliance program. This risk assessment will consist of identifying risks, mitigations, and monitoring mechanisms. The annual risk assessment will be submitted to the university compliance officer, EO, president and system compliance officer for review.

Possible Violations

Possible violations of United States export control laws or regulations will be investigated by CSI in coordination with the system RSO and/or the EO to the extent deemed necessary.

If through investigation, it is determined that any activity is not in compliance or may lead to noncompliance with export control laws and regulations, RSO and OGC will be notified immediately and the EO is authorized to suspend or terminate the activity.

Disciplinary Actions

While there are severe institutional and individual sanctions for violations of export controls laws, including the loss of research funding, loss of export privileges, as well as civil and criminal penalties including imprisonment, employees and students may also be subject to disciplinary action, up to and including dismissal, in accordance with system policies and regulations and Tarleton rules and procedures.

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 Parts 730-774 and 22 CFR Parts 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 Parts 730-774 and 22 CFR Parts 120-130 for further details.)

Deemed export – A release of technology or source code to a foreign person in the United States. A “deemed export” is considered an export to the country of nationality of the foreign person.

Defense article – Any item or technical data designated on the United States Munitions List. See ITAR, 22 CFR §121.1.

Defense service means:

- (1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles;
- (2) The furnishing to foreign persons of any technical data controlled under the USML (see 22 CFR §120.10), whether in the United States or abroad; or
- (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice. (See *also* 22 CFR§124.1.)

Dual-use – Items (i.e. commodity, software or technology) which are those having both commercial and military or proliferation applications.

End-user – The person abroad that receives and ultimately uses the exported or re-exported items. The end-user is not a forwarding agent or intermediary, but may also be the purchase or ultimate consignee (See 15 CFR772.1).

Export Control Classification Number (ECCN) – Number assigned to each specific category of items or technology listed specifically on the Commerce Control List maintained by the U.S. Department of Commerce, Bureau of Industry and Security. 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.

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 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, 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 visitor – Foreign persons having a residence in a foreign country, who are not employees or enrolled students of Tarleton, and are coming to Tarleton on a temporary basis as a result of a verbal or written agreement to host the foreign person by a faculty member, researcher, or administrator of Tarleton.

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, 22 CFR § 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 United States or abroad; or (iii) the application to situations abroad of personal knowledge or technical experience acquired in the United States.

System member(s) – Refers to all members of The Texas A&M University System.

Technology – Specific information necessary for the “development,” “production,” or “use” of a product. The information takes the form of “technical data” or “technical assistance.”

Controlled technology is defined in the General Technology Note and in the Commerce Control List (Supplement No. 1 to part 774 of the EAR).

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 (TAA) – An agreement for the performance of ITAR-controlled defense services or the disclosure of ITAR-controlled technical data. (22 CFR §120.22)

Technology Control Plan (TCP) – A technology control plan lays out the requirements for protecting export-controlled information and equipment for activities or research projects conducted at Tarleton. Tarleton has developed a [TCP template](#) for use on such projects.

Technical data – Includes information “required for” the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. It may take the form of 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 Tarleton 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.

List of Abbreviations

BIS	Department of Commerce Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity Jurisdiction
CSI	Tarleton Office of University Compliance and Strategic Initiatives
DDTC	Department of State Directorate of Defense Trade Controls
DFAR	Defense Federal Acquisition Regulation
EAR	Export Administration Regulations
FAR	Federal Acquisition Regulation
FRE	Fundamental Research Exclusion
ECCN	Export Control Classification Number
EO	Empowered Official
ITAR	International Traffic in Arms Regulations
MTA	Material Transfer Agreement
NDA	Non-Disclosure Agreement
OFAC	Department of the Treasury Office of Foreign Assets Control
OGC	Office of General Counsel, The Texas A&M University System
RPS	Restricted Party Screening
RSO	A&M System Research Security Office
SDN List	Specially Designated Nationals and Blocked Persons List
System	The Texas A&M University System
TAA	Technical Assistance Agreement
TCP	Technology Control Plan
TTC	Texas A&M Office of Technology Commercialization
USML	United States Munitions List