COMPLIANCE PROGRAM GUIDANCE MANUAL

EXPORT CONTROL

for

Texas A&M University-Victoria

COMPLIANCE PROGRAM GUIDANCE MANUAL

EXPORT CONTROL

for

Texas A&M University-Victoria

Responsible Office:
Academic Affairs/
Office of Research & Sponsored Programs

Revision History:
____

GENERAL | Export control laws and regulations are complex, fluid, dynamic, and fact-specific. Each proposed activity will be evaluated on a case–by–case basis.

GUIDANCE MANUAL BASIS | This guidance manual provides Texas A&M University-Victoria employees with basic educational content regarding export controls compliance and shall not be represented or construed as legal advice, nor relied upon exclusively. All questions must be directed to the Office of Research and Sponsored Programs (ORSP).

CONTENT:
EXPORT CONTROL COMPLIANCE PROGRAM GUIDANCE MANUAL

CONTENT: ... 3

EXPORT CONTROL COMPLIANCE PROGRAM GUIDANCE MANUAL ... 3

LIST OF ACRONYMS ... 5

SECTION 1.0 COMPLIANCE COMMITMENT ... 7

- WE'RE COMMITTED ... 7
- IT TAKES A TEAM ... 8
- WE'RE HERE TO HELP ... 8

SECTION 2.0 FEDERAL REGULATORY STATUTES AND REGULATIONS ... 9

- PREFACE ... 9
- DDTC - INTERNATIONAL TRAFFIC IN ARMS REGULATIONS ... 9
- BIS – EXPORT ADMINISTRATION REGULATIONS ... 12
- OFAC – SANCTION PROGRAMS ... 15
- PUTTING IT ALL TOGETHER – A HOLISTIC APPROACH ... 16

SECTION 3.0 KEY PARTNER IN COMPLIANCE – IT TAKES A TEAM ... 16

- INDIVIDUAL RESPONSIBILITY ... 16
- ENPOWERED OFFICIAL ... 17
- TITLE OF PRIMARY POINT OF CONTACT ... 17

SECTION 4.0 IDENTIFYING CONCERNS – KNOWING WHEN AND WHO TO CONTACT ... 18

- WHAT'S THE CONCERN ... 18
- CONTRACTUAL PROVISIONS OF CONCERN ... 19
- SPECIFIC PROVISIONS ... 20
- RESTRICTED PARTY SCREENINGS – KNOWING OUR CUSTOMERS ... 23
- RESOLVING RED FLAGS – WHO CAN HELP ... 23
- PREFACE – THE PILLARS OF AN EFFECTIVE PROGRAM ... 24

SECTION 5.0 OPERATING PROCEDURES ... 24

- SPONSORED RESEARCH ... 24
- AGREEMENTS (NON-SPONSORED) ... 25
- FINANCIAL TRANSACTIONS ... 25
- INTERNATIONAL TRAVEL ... 26
- EMPLOYMENT ... 28
- SHIPMENTS ... 28

TECHNOLOGY COMMERCIALIZATION 29
TECHNOLOGY CONTROL PLANS 29
GOVERNMENTAL APPLICATIONS & LICENSING 31
TRAINING 31
RECORDKEEPING 31
INTERNAL MONITORING 32
POSSIBLE VIOLATIONS & DISCIPLINARY ACTIONS 32
6.0 RELATED STATUTES, POLICIES, OR REQUIREMENTS 33
FEDERAL 33
LOCAL 33
7.0 CONTACT INFORMATION 34

LIST OF ACRONYMS

AECA	Arms Export Control Act
AES	Automated Export System
AFMC	Air Force Materiel Command
ARL	Army Research Laboratory
BIS	Bureau of Industry and Security
CCL	Commerce Control List
CJ	Commodity jurisdiction
CIO	Chief Information Officer
DEAR	Department of Energy Acquisition Regulation
DDTC	Department of State's Directorate of Defense Trade Controls
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
EAR	Export Administration Regulations
ECRA	Export Control Reform Act of 2018
EO	Empowered Official
FMO	Financial Management Operations
FRE	Fundamental Research Exclusion
FTR	Foreign Trade Regulations
IEEPA	International Emergency Economic Powers Act
ITAR	International Traffic in Arms Regulations
NIST	National Institute of Standards and Technology
NSPM-33	National Security Presidential Memorandum
NSDD	National Security Decision Directives
OAC	Office of Antiboycott
OGC	Office of General Counsel
OFAC	Department of the Treasury's Office of Foreign Assets Control

ORSP	Office of Research and Sponsored Programs
RPS	Restricted Party Screenings
RSO	Research Security Officer
SDN	Specially Designated Nationals
SP	Special Publication
TCP	Technology Control Plan
TEA	Trading with the Enemy Act
TRA	Tax Reform Act
TWEA	Trading with the Enemy Act
USG	U.S. government
USML	U.S. Munitions List
UVL	Unverified List

SECTION 1.0 COMPLIANCE COMMITMENT

WE'RE COMMITTED

Texas A&M University-Victoria (A&M-VICTORIA) is committed to upholding the highest standard of ethical conduct and compliance with its legal obligations, including federal statutes and regulations implementing U.S. export control policies. A&M-Victoria, a dynamic destination institution serving Texas and the world, is dedicated to providing every student with educational and leadership opportunities to become a successful professional and engaged global citizen.

The U.S. government (USG) administers strategically driven laws and regulations controlling certain exports and re–exports. Through the Arms Export Control Act (AECA), the International Emergency Economic Powers Act (IEEPA), the Trading with the Enemy Act (TEA), the Export Control Reform Act of 2018 (ECRA), and other legislation, the USG regulates exports of items, technologies, software, and services to protect U.S. national and economic security. National Security Presidential Memorandum 33 (NSPM-33) was issued as a necessity to protect U.S.–funded scientific research from foreign interference and exploitation on the U.S.-based research ecosystem, with export control compliance serving as a foundational component of required research security programs. Purposes of export control laws and regulations include:

- preventing the transfer of sensitive items and technology that could cause harm the U.S. or its allies' interests;
- achieving a balance in safeguarding sensitive interests and the economic value of exports;
- implementing U.S. foreign policy or domestic political concerns;
- implementing sanctions as a policy alternative or supplement to either diplomacy or way; and
- furthering multi-lateral agreement policies where the U.S. participates.

"U.S. Persons"—as defined in various regulations implementing export control laws (i.e. 15 C.F.R. § 772.1 and 22 C.F.R. § 120.15)—are required to comply with these laws. The definition of "U. S. Persons" under these regulations generally include: any individual granted U.S. citizenship; any individual granted U.S. permanent residency; any individual granted "protected person" under 8 U.S.C. 1324b(a)(3); any entity incorporated in the U.S. under U.S. law; and any facet of the USG.

IT TAKES A TEAM

Export control compliance necessitates a team effort to mitigate potential violations. A&M-Victoria employees must maintain open communication channels with their supervisors, unit heads, and ORSP to achieve the highest level of ethical standards and compliance. All employees must understand that export control statutes and regulations apply broadly, not just to those activities that can be construed as national security efforts. This A&M-Victoria Export Control Compliance Program Guidance Manual is designed as a first line of assistance for all employees to support export control compliance. The guidance manual supplements the required member rule, *15.02.99.J1, Export Control Program Management*, and the resulting scope is to guide in properly obtaining required administrative approvals for export control-related compliance. To the extent the guidance manual conflicts with *System Policy 15.02* or *System Rule 15.02.99.S1*, the System Policy supersedes.

WE'RE HERE TO HELP

Any questions regarding export control compliance shall be directed to ORSP:

Texas A&M University-Victoria

EXPORT CONTROL

University West Suite 272
Research and Sponsored Programs | Texas A&M University-Victoria
| 361-570-4374 | RSP@A&M-Victoria.edu

SECTION 2.0 FEDERAL REGULATORY STATUTES AND REGULATIONS

PREFACE

Through the Arms Export Control Act (AECA)[1], the International Emergency Economic Powers Act[2] (IEEPA), the Trading with the Enemy Act (TEA), the Export Control Reform Act of 2018 (ECRA)[3], and other legislation, the USG administers programs related to export control legislation. These related laws and regulations are strategically driven for purposes of national and economic security. Although there are more than 20 USG federal agencies that administer programs related to export controls legislation, this guidance manual focuses primarily on the Department of State's Directorate of Defense Trade Controls (DDTC), the Department of Commerce's Bureau of Industry and Security (BIS), and the Department of Treasury's Office of Foreign Assets Control (OFAC) [4].

In addition to establishing laws and regulations that implement the USG's policy regarding export controls, there are various enforcement mechanisms by which the USG ensures compliance with such laws and regulations. Both criminal and civil penalties for export control violations can be severe. For violations of the International Traffic in Arms Regulations (ITAR), statutes authorize criminal penalties in excess of $1 million per violation or twice the transaction value and can include imprisonment. Violations of the Export Administration Regulations (EAR) can be subject to fines in excess of $300,00 or twice the transaction value and can include denial of export privileges. Because of the dynamic and fluid nature of export control legislation and associated penalties for non-compliance, all A&M-VICTORIA employees must understand the nature of their work and the potential for applicability to these laws and regulations. ORSP can assist any A&M-VICTORIA employee in determining the applicability to these laws and regulations.

DDTC - INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

Under the AECA, the Department of State DDTC implements the ITAR (22 C.F.R. § 120-129), regulating exports of goods, services, software, and technical data for use primarily in military applications. It is important to note that items specifically included in this set of legislation are considered "defense articles" or "defense services." ITAR §120.3 describes the policy on designating or determining "defense articles" and "defense services" subject to the U.S. Munitions List (USML) that is described in ITAR §121.1. The USML regulates such defense articles, software, and services. Specifically, these terms corresponding to the USML are defined in the ITAR:

- ITAR § 120.6 "Defense Article"

  Generally, a "defense article" means any item or technical data designated on the USML (ITAR §121.1) including technical data recorded or stored in any physical form, models, mockups, or other items that reveal technical data directly relating to items designated in §121.1. Further, this definition also includes forgings, castings, and other unfinished products that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles. This definition does not include basic marketing information on function or purpose or general system descriptions.

- ITAR § 120.9 "Defense Service"

[1] Arms Export Controls Act | 22 U.S.C 2778
[2] International Emergency Economic Powers Act | 50 U.S.C. 1701
[3] National Defense Authorization Act for 2019 | Public Law No: 115-232
[4] Office of Foreign Assets Control (OFAC) | 31 C.F.R. § 500-599

The ITAR definition of “defense service” includes three components. Generally, a “defense service” is the furnishing of assistance (to include training) to foreign persons, whether abroad or in the U.S. in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of “defense articles”; the furnishing of any technical data controlled to foreign persons whether in the U.S. or abroad; or providing military training of foreign units and forces while in the U.S. or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

- ITAR § 120.11 “Order of Review”

  Articles are controlled on the USML because they are either enumerated in a category or described in a “catch-all” paragraph that incorporates “specially designed” as a control parameter. In order to classify an item on the USML, begin with a review of the general characteristics of the item. In all cases, articles not controlled on the USML may be subject to another USG regulatory agency (see § 120.5 and Supplement No. 4 to part 774 of the Export Administration Regulations for guidance on classifying an item subject to the EAR).

- ITAR § 120.34 “Public Domain”

  Public domain means information that is published and that is generally accessible or available to the public: through sales at newsstands and bookstores; through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; through second class mailing privileges granted by the USG; at libraries open to the public or from which the public can obtain documents; through patents available at any patent office; through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States; through public release in any form after approval by the cognizant USG department or agency; through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is considered basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific USG access and dissemination controls. University research will not be considered fundamental research if the university or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or if the research is funded by the USG and specific access and dissemination controls protecting information resulting from the research are applicable.

- ITAR § 120.33 “Technical Data”

  Generally, the term “technical data” as defined in the ITAR means information other than software defined in § 120.10(a)(4) that is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of “defense articles.” This also includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation. It also includes classified information relating to defense articles and defense services on the USML and 600-Series on the Commerce Control List (CCL), information covered by a secrecy order; or software directly related to defense articles.

- ITAR § 121.1 “U.S. Munitions List”

  Articles, services, and related technical data are designated as “defense articles” or “defense services” pursuant to sections 38 and 47(7) of the AECA. Categories of the USML are organized by paragraphs and subparagraphs alphanumerically. Generally, these items and information are enumerated or describe end–items, followed by major systems and equipment; parts, components, accessories and attachments; and technical data and defense services directly related to the defense articles of that particular USML category. Categories of the USML are as follows:

- Category I — Firearms and Related Articles
- Category II — Guns and Armament
- Category III — Ammunition/Ordnance
- Category IV — Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, & Mines
- Category V — Explosives & Energetic Materials, Propellants, Incendiary Agents, & Their Constituents
- Category VI — Surface Vessels of War and Special Naval Equipment
- Category VII — Ground Vehicles
- Category VIII — Aircraft and Related Articles
- Category IX — Military Training Equipment and Training
- Category X — Personal Protective Equipment
- Category XI — Military Electronics
- Category XII — Fire Control, Laser, Imaging, and Guidance Equipment
- Category XIII — Materials and Miscellaneous Articles
- Category XIV — Toxicological Agents, Including Chemical Agents, Biological Agents, & Assoc. Equipment
- Category XV — Spacecraft and Related Articles
- Category XVI — Nuclear Weapons and Related Articles
- Category XVII — Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
- Category XVIII — Directed Energy Weapons
- Category XIX — Gas Turbine Engines and Associated Equipment
- Category XX — Submersible Vessels and Related Articles
- Category XXI — Articles, Technical Data, and Defense Services Not Otherwise Enumerated

- ITAR § 120.62 "U.S. Person"

  Under the ITAR, "U.S. Person" means a person who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). Additionally, it also includes federal, state, and local governmental entities, and any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to conduct business in the U.S.

An item might be classified as a defense article if it was developed for the military or if it could have a significant military application. Understanding that a defense article can be purchased or have widespread civilian use is essential. This fact does not exempt the defense article from being subject to the ITAR. Regarding technology subject to the ITAR, a defense service is generally considered furnishing assistance, including training, to non-U.S. persons related to the design, development, maintenance, or use of defense articles. Further, under the ITAR, a deemed export includes disclosing or transferring technical data to a non-U.S. person, whether in the U.S. or abroad.

Beyond controls of goods and services, DDTC administers the "Debarred Parties" list (ITAR § 127.7). These individuals and entities are prohibited from participating directly or indirectly in the export of defense articles or defense services (ITAR § 126.1) and there is a presumption of denial for requested export licenses. Additionally, it is the policy of the United States to deny licenses and other approvals for exports and imports of defense articles and defense services, destined for or originating in certain countries. Specific policies of denial for these "proscribed countries" are articulated in ITAR § 126.1. Exporters of defense articles and defense services are required to register with DDTC.

HOW MIGHT A&M-VICTORIA BE AFFECTED?

“Fundamental research” is not a stand-alone term defined within the ITAR; rather, it is embedded within the definition of “public domain.” Additionally, given the precedence set in § 121.1(b), reviews as to if an item is subject to the ITAR or EAR should always start with a review of the ITAR. Withstanding the limited licensing exceptions available under the ITAR, any “defense article” or “defense service” requires a license to be exported or temporarily imported. All persons or entities engaged in the manufacture, export, or brokering of “defense articles” and “defense services” are required to be registered with the Department of State. Because of the nature of work at A&M-Victoria, the Provost and VP for Academic Affairs, an empowered official (EO), has determined that such registration is necessary at this time in the event A&M-Victoria needs to apply for a license or agreement for approval from DDTC.

Some precision devices, such as night vision goggles and infrared cameras, utilized at an institute of higher education in the course and scope of educational activities or fundamental research, might be subject to the ITAR. The fact that A&M-Victoria employees can procure “defense articles” commercially does not prevent the “defense article” from being subject to ITAR restrictions. Because of this, it is essential to determine if an item or information is subject to the ITAR before any incorporation into laboratories or educational activities.

BIS – EXPORT ADMINISTRATION REGULATIONS

Under the ECRA, the Department of Commerce BIS administers the EAR (15 C.F.R. § 730-774), regulating exports and re-exports of dual-use goods, software, and technology. BIS also administers and enforces regulations prohibiting specific trade and transactions with countries, entities, and individuals by U.S. persons or from the U.S. under the TEA and IEEPA. As a component of the EAR, the Commerce Control List (CCL) enumerates thousands of goods, software, and technology, which are subject to varying degrees of export restrictions, dependent upon the designated export control classification number (ECCN). The EAR also imposes certain end-use controls described in 15 C.F.R. § 744. Most items and some information found at institutions of higher education are subject to the EAR. The following EAR definitions are of interest in determining when a license may be needed for certain activities:

- EAR § 774 “Commerce Control List (CCL)”

  The CCL comprises a list of items under the jurisdiction of the BIS. If goods, software, or technology are subject to the jurisdiction of the BIS, but not enumerated on the CCL, they are designated EAR99. The CCL categories are:

  - Category 0 — Nuclear Materials, Facilities, and Equipment [and Miscellaneous Items]
  - Category 1 — Special Materials & Related Equip., Chemicals, “Microorganisms,” & “Toxins”
  - Category 2 — Materials Processing

- Category 3 Electronics
- Category 4 Computers
- Category 5 Part 1 Telecommunications
- Category 5 Part 2 Information Security
- Category 6 Sensors and Lasers
- Category 7 Navigation and Avionics
- Category 8 Marine
- Category 9 Aerospace and Propulsion

The CCL product groups include:

- Group A Systems, Equipment, and Components
- Group B Test, Inspection, and Production Equipment
- Group C Materials
- Group D Software
- Group E Technology

- EAR § 772 “Dual–Use”

  Items that have both commercial and military or proliferation applications. Goods, software, and technology that are considered “dual-use” are those that can be used in both military and civil applications. Such items may be restricted for export control purposes.

- EAR § 772 “Export Control Classification Number” (ECCN)

  The ECCN consists of a set of digits and a letter, categorized by category (numeric) as the first digit, and product group (alpha) as the second. The remaining three digits are numerical, further categorizing the goods, software, or technology on the CCL.

- EAR § 734.8 “Fundamental Research”

  Research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.

- EAR § 734.7 “Published”

  “Technology” or “software” is not subject to the EAR when it has been made available to the public without restrictions upon its further dissemination.

- EAR § 772 “Use”

  Operation, installation, maintenance, repair, overhaul, and refurbishing. For some technology ECCNs, “use” as defined must be met before a potential deemed export license might be needed. However, it is important to note that some technology ECCNs include only some components of “use” as potentially requiring a deemed export license.

- EAR § 772 "U.S. Person"

  Unless specifically enumerated in other parts of the EAR (such as §740.9, 740.14, 740.21(f)(2), 746, and 760), the term "U.S. Person" includes any individual who is a citizen of the United States, permanent resident alien of the United States, or protected individual as defined by U.S.C. 1324b(a)(3). It also includes any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and any person in the United States. When goods, software, or technology are determined to be controlled under the EAR and an applicable ECCN has been properly established, the related controls can then be derived based upon the BIS Country Chart (Supplement No. 1 to Part 738). For example, an item controlled to country A might not be controlled to country B under the EAR. Additionally, a release of controlled technology to a non-U.S. person in the U.S. is considered a "deemed export," because it is considered to be an export to the individual's country of most recent citizenship.

In addition to any controls placed on dual-use goods, software, or technology through the CCL, the EAR imposes specific catch-all, end-use and end-user controls, prohibiting exports, re-exports, and selected transfers to certain end users and end uses, unless authorized by BIS (15 C.F.R. § 744). Performance of services in furtherance of these defined end-uses are also generally prohibited. These restricted end-uses include proliferation activities such as chemical and biological weapons, missiles, nuclear weapons, certain encryption, sensitive nuclear activities, and certain military end-uses.

Additionally, BIS incorporates the Office of Antiboycott Compliance (OAC), which is charged with administering the Antiboycott Laws. These laws discourage and may prohibit U.S. persons from supporting international boycotts. The Tax Reform Act (TRA) shares a common purpose.

These laws also have the effect of preventing U.S. persons from being used to implement foreign policies of other nations, which are in opposition of U.S. policy. In addition to compliance with these laws, some actions might be reportable. For example, the EAR requires U.S. persons to report quarterly any requests they have received to comply with, further, or support an unsanctioned international boycott. Contracts and agreements should be fully reviewed for conditions of participation in such international boycotts.

HOW MIGHT A&M-VICTORIA BE AFFECTED?

Most goods, software, or technology at an institute of higher education might be subject to the EAR. In the case of technology, information released through "fundamental research" is generally not subject to the EAR. It is important to note that goods and software are not released from controls under the EAR through fundamental research. The mere fact that University/Agency employees can procure "dual-use" goods, software, and technology commercially does not eliminate the item or information from being subject to EAR restrictions.

OFAC – SANCTION PROGRAMS

Promulgated under various acts, executive orders, and presidential national emergency powers, including but not limited to the IEEPA and Trading with the Enemy Act (TWEA)[5], amongst many others, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) administers, interprets, and enforces U.S. economic embargos and sanctions (31 CFR 500-599), with many of the sanctions being multilateral in scope, based on United Nations and other international mandates involving close cooperation with other allied governments. The general scope of such embargoes or sanctions is to further U.S. foreign policy interests and national security goals against certain targeted countries, regimes, terrorists, international narcotics traffickers, individuals engaged in activities that are related to the proliferation of weapons of mass destruction, as well as other threats to the national security, foreign policy, or economy of the U.S. Generally, these sanction programs prohibit U.S. persons from engaging in commercial transactions with parties in the embargoed or sanction countries, with certain limited exceptions.

OFAC imposes controls on transactions and freezes assets under U.S. jurisdiction. The Department of Treasury has a significant history in administering sanctions. Sanction programs can be comprehensive or selective, implementing the blocking of assets and trade restrictions. OFAC sanction programs and lists can be country, individual, or entity-specific. Sanctions can be comprehensive or limited in nature. Comprehensive sanctions prohibit U.S. persons from engaging in broad commercial activities with persons in the embargoed country, including but not limited to exports, imports, provisions of services, payment, investment, or other financial transactions. Examples of comprehensive sanction programs include, but are not limited to, Iran, North Korea, certain regions in Ukraine, and Cuba. U.S. persons are generally prohibited, with certain exceptions, from many transactions unless authorized through a general or specific license from OFAC. Limited sanctions generally prohibit U.S. persons from engaging with specific activities under sanctions for countries or programs but may be free from licensing obligations for activities not subject to the particular sector and with individuals in that country. At the time of this publication, an example of limited sanctions programs includes Afghanistan-related sanctions.

Further, OFAC maintains list-based sanction programs on entities and persons. The OFAC "Specially Designated Nationals" (SDN) list incorporates individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries, as well as incorporating individuals, groups, and entities such as terrorists or narcotics traffickers designated under sanctioning programs that are not country-specific. U.S. persons are generally prohibited from conducting business with SDNs anywhere in the world without a license from OFAC. For example, if a company based in France is partially owned by individuals in Australia, and the entity is placed on the SDN list, U.S. persons cannot conduct business with the entity without obtaining a specific license from OFAC. Thus, it is imperative to know your customer before moving forward with any transaction.

HOW MIGHT A&M-VICTORIA BE AFFECTED?

OFAC-administered regulations and the EAR or ITAR have overlapping jurisdiction regarding embargoed countries, with the OFAC-administered regulations generally having primary jurisdiction. There is potential for some case-specific scenarios to require a license from OFAC, from BIS, or both. For example, A&M-VICTORIA might offer distance education courses where information and materials are not subject to either the EAR or the ITAR. However, ORSP would need to

[5] Trading With the Enemy Act | 50 U.S.C §§ 1-44

review those who register for the course, and their physical location outside of the U.S., to determine if any OFAC sanctions program is applicable at that time.

PUTTING IT ALL TOGETHER – A HOLISTIC APPROACH

With a complicated regulatory body of law spanning many federal agencies, it is essential to recognize that many facets are needed for a holistic approach to effective export control compliance. The pillars of an export control compliance program include: a commitment to compliance from management; a continuous risk assessment of the export control ecosystem; a formal written management and compliance program; continuous training; a holistic approach assessing all facets of export control compliance from initial setup to final post activity closeout; adherence to recordkeeping and regulatory compliance; internal and external monitoring including audit; internal program for administration of compliance violations; and an internal program for completing appropriate corrective actions. A holistic risk-based approach in the development of compliance procedures is essential in maintaining an effective export control compliance program. Open communication channels within A&M-VICTORIA and beyond with the members are pillars of the A&M-VICTORIA export controls compliance program.

SECTION 3.0 KEY PARTNER IN COMPLIANCE – IT TAKES A TEAM

INDIVIDUAL RESPONSIBILITY

All A&M-VICTORIA employees play a crucial role in promoting a culture of export control compliance and will conduct their scope of employment in accordance with U.S. export control laws and regulations and A&M-VICTORIA rules and procedures while being aware of and responsible for the export control implications associated with their work and institutional responsibilities. To balance global engagement and compliance with export control laws and regulations, A&M-VICTORIA employees must be familiar with such, including essential export control exemptions and exceptions, and how they relate to their institutional responsibility. ORSP is available to assist all employees in navigating the export control laws and regulations.

Violations can be severe, directly affecting the A&M-VICTORIA employee through fines, loss of funding, loss of export privileges, and or personal criminal liability. All A&M-VICTORIA employees should:

- understand their export control obligations and participate in regular training to help identify

  export control concerns;
- be aware of export control-related red flags;
- determine—*prior to the activity*—whether any information or technology involved in the activity is subject to export control regulations;
- periodically review their educational activities for continuing internal compliance monitoring;
- report suspected or known violations to the A&M-VICTORIA EO or via the Ethics Point Hotline; and
- know to contact ORSP with any export control-related questions.

ENPOWERED OFFICIAL

The Provost and V.P. for Academic Affairs serves as the A&M-VICTORIA EO for all purposes related to applicable federal export control laws and regulations. The EO is responsible for obtaining approvals required for compliance with export control laws and regulations. All export license applications, commodity jurisdiction (CJ) requests, and/or Commodity Classification Automated Tracking System (CCATS) requests must be submitted in consultation with the System RSO and through the System's DDTC registration. The Director of Research and Sponsored Programs serves as the A&M-VICTORIA point of contact for export control matters. The EO is responsible for compliance with export control laws and regulations. Further, the EO is the A&M-VICTORIA official authorized to sign license applications and other authorizations required by export control laws and regulations on behalf of A&M-VICTORIA. Pursuant to System Policy 15.02, *Export Control Program Management*, ORSP is the designated office through the A&M-VICTORIA EO in communicating with federal regulatory bodies during investigations. A&M-VICTORIA employees are to report suspected or known violations to the A&M-VICTORIA EO and will maintain their commitment to promoting a culture of compliance with all associated laws, regulations, policies, rules, and procedures.

TITLE OF PRIMARY POINT OF CONTACT

The Director of Research and Sponsored Programs is responsible for implementing and monitoring risk mitigation and maintaining and updating this manual. In accordance with System Policy 15.02, the A&M-VICTORIA regularly participates in the System Export Control Affinity Group and consults System OGC accordingly. Of utmost importance, the Director of Research and Sponsored Programs serves as the A&M-VICTORIA resource for all export control-related matters.

Accordingly, ORSP is responsible for day-to-day procedures implementing the A&M-VICTORIA export control program, including:

- implementation, oversight, and monitoring;
- establishment of a centralized data storage system for export control-related determinations;
- assisting A&M-VICTORIA employees with export control determinations;

- serving as the primary export control contact for A&M-VICTORIA; and

- investigating potential or known violations.

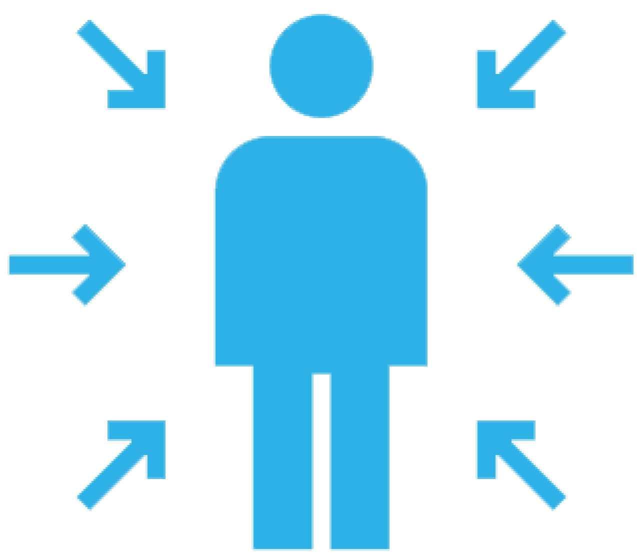
A&M-VICTORIA encourages its employees to establish global engagements in the pursuit of mutually beneficial fundamental scientific inquiry, cultural, or educational opportunities. These activities strengthen the academic and research programs and are fundamental to each member's educational system.

However, before engaging in any external activity (including, but not limited to: collaborations for publication, funded or unfunded research projects, external employment, foreign travel, etc.) involving individuals or entities located in a Country of Concern, a request must first be submitted to the System RSO for review in accordance with System Regulation 15.05.04, *High Risk Global Engagements and High Risk International Collaborations*, and approval must be obtained through that process ***before*** engaging in the external activity.

SECTION 4.0 IDENTIFYING CONCERNS – KNOWING WHEN AND WHO TO CONTACT

WHAT'S THE CONCERN

A&M-VICTORIA's business functions can be impacted by export control-related compliance. Identifying potential red flags and knowing whom to contact for help is paramount in navigating your work's potential export control implications at the A&M-VICTORIA. This distinction serves as another pillar of an effective export control compliance program. The following indicators serve as potential areas of concern that might contain export control-related implications for the A&M-VICTORIA business. Please be aware that this list serves as a guide and is not entirely comprehensive. Remember that ORSP is here to help you navigate the potential export control implications of your work at A&M-VICTORIA.



- The results of research or educational activities are intended for military purposes, dual-use (military and civilian purposes), or for other restricted end-uses or end-users.

- Non-U.S. persons will have access to controlled physical items or facilities.

- Software that includes encryption features will be developed or purchased.

- A&M-VICTORIA employees will export or travel abroad with equipment, items, or technical information, including supplies to conduct trainings, chemicals, biological materials, encrypted software, or other controlled physical items; or travel abroad with electronic devices containing controlled information.

- A transaction is proposed with embargoed countries or entities, individuals or entities located in embargoed countries, or those who are prohibited end-users, or for activities that are prohibited end-uses.

- A contractual obligation requires pre-approval rights to publication or restricts the participation of non-U.S. persons.
- Distance education materials will be provided to an individual located in an embargoed country.
- The activity requires a physical export.
- Proprietary invention disclosures are created from the educational activity.

The BIS publishes "Red Flag Indicators," which includes the following:

- "The customer or its address is similar to one of the parties found on the Commerce Department's [BIS'] list of denied persons.
- The customer or purchasing agent is reluctant to offer information about the end–use of the item.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- The customer has little or no business background.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.
- Routine installation, training, or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- Packaging is inconsistent with the stated method of shipment or destination.
- When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for reexport."

Further, BIS publishes "Know Your Customer Guidance," which provides information related to understanding prohibited end-uses and end-users.

CONTRACTUAL PROVISIONS OF CONCERN

It is understood that most data and information involved in the course and scope of A&M-VICTORIA activities could be excluded from export control regulations under the ITAR or the EAR based on several key exclusions, including the public domain or publicly available exclusion, or the fundamental research exclusion. A&M-VICTORIA employees must be aware of these key exclusions and understand that the privileges afforded by such exclusions can be voided if certain provisions are present in contractual obligations. For example, restrictions on the dissemination of research results or restrictions on the participation of non-U.S. persons can negate these key exclusions. These activities may warrant licensing requirements or undertaking additional monitoring to mitigate associated risk. Additionally, it is also important to understand that although the data or information may not be subject to regulatory bodies, OFAC sanctioning programs are mutually exclusive of these exemptions and should be taken into consideration. Simply stated, restrictions administered by OFAC are not affected by exclusions available under the ITAR or the EAR. For example, providing course materials via distance education to an individual who is on the SDN list is most likely subject to OFAC licensing. It is important to note that the fundamental research exclusions apply to information, and not tangible items or technology otherwise protected under the EAR or ITAR. If any of the following contractual provisions are present within a contract or agreement, the agreement should be further reviewed prior to execution of the agreement:

- The customer retains the right to restrict or approve of any publications or dissemination of activity results (excluding a standard customary brief delay to protect confidential, proprietary, or patentability details of an invention).
- The customer retains the right in ownership of the data derived from the activity.
- Statements regarding export control laws and regulations applying to the activity.
- Incorporation by reference of Federal Acquisition Regulations (FARs), USG agency-specific FARs, or other USG regulations that impose specific controls or access to or dissemination of the activity results.
- Restrictions or prohibitions against activity personnel based upon citizenship or natural origin.
- Statements indicating the customer intends to provide export-controlled items or information for use in the activity.
- A prototype or software is required as a deliverable of the activity.
- The activity will involve the use of export-controlled items or information obtained from a third party.
- The activity will take place outside the U.S.

SPECIFIC PROVISIONS

Specific contractual provisions should be considered as potential risk indicators in negating exclusions of export control laws and regulations related to the results of the activity. Language may be incorporated within the contract as reference and might be stipulated to be included as part of a prime contract or flowed down to a subcontract. These contractual clauses of concern can include, but are not limited to:

- **FAR 52.227-14 (*Rights in Data—General*)**

  This particular clause grants the USG unlimited rights in data first produced or delivered under the contract. USG 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. Alternate IV can be suggested for basic or applied research, which will provide the contractor with the right to copyright data without USG permission.

- **FAR 52.227-17 (*Rights in Data—Special Works*)**

  This particular clause prevents the release, distribution, and publication of any data originally produced for the USG's internal use and represents an absolute restriction on the publication or dissemination of the contractor-generated data. It should not apply to basic and applied research, thus should be requested to be removed on the basis of exceptions to the clause's applicability.

- **FAR 52.204-21 (*Basic Safeguarding of Covered Contractor Information Systems*)**

  This clause requires additional IT security controls if controlled information is exchanged during the course of the contract. There is a chance that this research may also be export-controlled.

- **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; or (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. You may also refer to IRS Ruling 76-296 or 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." The Principal Investigator (PI) may be required 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 clause is commonly found in contracts involving Controlled Technology and sponsored by military agencies. The PI may be required to certify that no Foreign Nationals will be working on the project. If no Foreign Nationals will be participating on the project, this clause may not be applicable.

- **ARL 52.005-4401 (*Release of Information*)**

  Includes reference to "non-releasable, unclassified information" and requires the contractor to "confer and consult" with the sponsor prior to release of information. The sponsor retains publication/information approval, which voids the FRE. Contract Negotiators may wish to 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 5353.227-9000 (*Export–Controlled Data Restrictions*)**

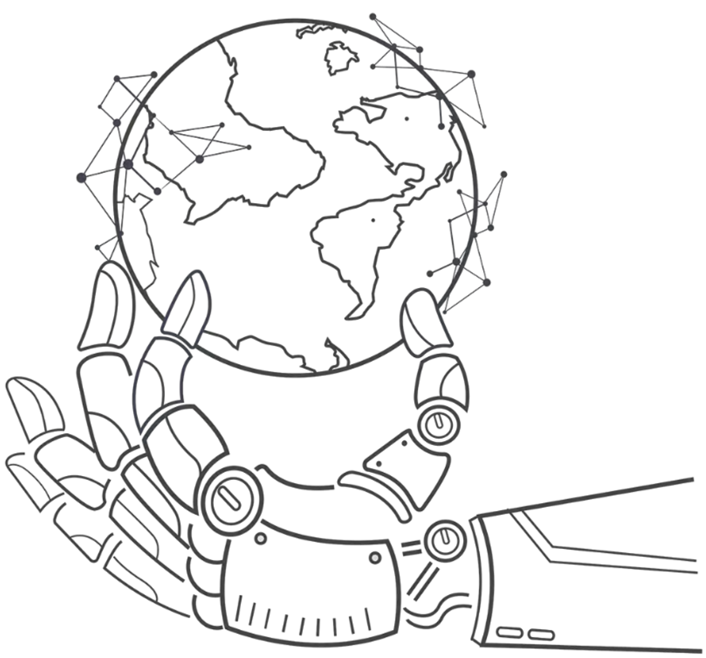
An export license is required prior to assigning any Foreign National to work on the project or allowing Foreign Nationals access to the work, equipment, or technical data generated by the project. Foreign Nationals make up a large portion of the contractor's scientific undergraduate, graduate, post-doctoral, and visiting scholar population. Many students depend on these projects to complete their thesis or dissertation. Students may need to ask the PI if the project is basic or applied research. If so, the project may fall under an ITAR exclusion. The PI may also ask the defense contractor if foreign students are allowed to work on the project. If yes, obtain confirmation in writing.

- **AFMC 5352.227-9000 (*Equipment and Technical Data Generated Controlled by ITAR*)**

  This clause requires an export license prior to assigning any foreign national to work on the project or allowing foreign persons access to the work, equipment or technical data generated by the project.

- **DFARS 252.227-7025 (*Limitations on the Use or Disclosure of Government–Furnished Information Marked with Restrictive Legends*)**

  This clause implements restrictions on the use or disclosure of certain information furnished by the government. This may not always be an export control concern, but the contractor is required to ensure that all project personnel are aware of and following the government's restrictions on this information.



- **DEAR 952.204-71 (*Sensitive Foreign Nations Controls*)**

  This is a foreign national restriction and voids the Fundamental Research Exclusion (FRE). When the sponsor includes this clause, they are required to attach a list of countries that they consider to be "Sensitive Nations."

- **DFAR 252.204-7008 (*Compliance with Safeguarding Covered Defense Information Controls*)**

  This clause states the contractor must implement the same security requirements required by DFAR clause 252.204-7012 for all covered defense information on all covered contractor information systems that support the performance of this contract. If the contractor proposes to vary from any of the NIST requirements, a written explanation must be submitted to the Department of Defense (DoD), Chief Information Officer (CIO), either as to why the requirement is inapplicable or how an alternative but equally effective measure will be used.

- **DFAR 252.204-7009 (*Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information*)**

  This clause prohibits third party contractors who are assisting with assessments of cyber incidents from unauthorized release or disclosure. The contractor agrees that the conditions listed on the clause must apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFAR clause 252.204-7012. This is a publication restriction and voids the FRE.

- **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, 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 the DoD.

RESTRICTED PARTY SCREENINGS – KNOWING OUR CUSTOMERS

Restricted party screenings (RPS) are conducted on non-U.S. persons as a risk-based mitigation strategy to reduce the likelihood of potentially committing an export control or sanction/embargo violation. If transactions are not wholly prohibited, licenses are most likely required for carrying out transactions with prohibited or restricted end-users. OFAC's denial lists are screened against to reduce the likelihood of providing a service to an individual that is a denied person or affiliated with a denied entity or government, or to an individual that is from a country that is comprehensively sanctioned or embargoed, and thus such service could be licensable under OFAC sanctioning programs, whether list or country-based. OFAC targets foreign countries, regimes, individuals, and entities based upon U.S. foreign policy and national security goals. Collectively, OFAC designates these individuals as SDNs, and U.S. persons are generally prohibited from conducting business without a specific license. BIS administers the "Denied Persons List," the "Entity List," and the "Unverified List." The "Denied Persons List" prohibits any listed person from participating in any component of an export transaction. The "Entity List" comprises of certain non-U.S. persons (including businesses, research institutions, government organizations, private organizations, individuals, universities, etc.) subject to licensing requirements for export, reexport, and transfer of certain items and information subject to the EAR. Parties listed on the Unverified List (UVL) are ineligible to receive items subject to the Export Administration EAR by means of a license exception. In addition, exporters must file an Automated Export System (AES) record for all exports to parties listed on the UVL and obtain a statement from such parties prior to exporting, reexporting, or transferring to such parties any item subject to the EAR which is not subject to a license requirement. DDTC administers the "Debarred Parties" list. These individuals and entities are prohibited from participating directly or indirectly in the export of defense articles or defense services. Additionally, DDTC administers a proscribed countries list (22 CFR § 126.1) of specific countries that are subject to arms embargoes.

Pursuant to compliance with these requirements, ORSP conducts RPS as a risk–based methodology in identifying activities subject to these controls or licensing requirements. These efforts help mitigate the risk of A&M-VICTORIA conducting business with entities or individuals that have been debarred, denied export privileges, or are otherwise contained within a USG restricted parties list. ORSP has licensed export control related software permitting authorized users to conduct RPS electronically and collectively, without having to separately visit various USG web sites that administer such sanctioning programs individually.

RESOLVING RED FLAGS – WHO CAN HELP

When potential export control red flags are identified, ORSP should be consulted, who will then work with the involved parties in determining a commensurate course of action. In most cases, a license will not be required. However, ORSP can determine:

- if the conditions of the event merit a license application or other authorization;
- if the conditions of the event are such that an exclusion or license exception may be applicable; and/or
- if a technology control plan (TCP) or other requirements for the conduct of the activity are warranted to prevent unauthorized exports, whether deemed or physical.

The parties involved will work collaboratively to resolve the red flags.

PREFACE – THE PILLARS OF AN EFFECTIVE PROGRAM

The pillars of an effective export control compliance program include: a commitment to compliance from the management; a continuous risk assessment of the A&M-VICTORIA export control ecosystem; a formal written management and compliance program; ongoing training; a holistic approach to assessing all facets of export control compliance from initial setup to final post activity closeout; adherence to recordkeeping and regulatory compliance; internal and external monitoring including audit; internal program for administration of compliance violations; and an internal program for completing appropriate corrective actions.

A&M-VICTORIA applies a proactive and holistic approach in mitigating potential export control control-related risks. The first pillar of this approach includes completing an annual export control-specific risk assessment. The System RSO has developed a standardized tool that implements federal guidance for effective export control compliance programs. This tool is available to all System members to build effective risk-based strategies and efficiencies. To support a consolidated effort, A&M-VICTORIA is committed to complying with all applicable U.S. export control statutes and regulations. Export control statutes and regulations are complex, fluid, and dynamic. Thus, potential export-controlled activities will be evaluated on a case-by-case basis.

SECTION 5.0 OPERATING PROCEDURES

SPONSORED RESEARCH

ORSP administers sponsored research agreements on behalf of A&M-Victoria. ORSP has developed detailed internal export control program procedures concerning restricted party screenings and identification of potential export control-related activities. A&M-VICTORIA utilizes Maestro compliance module to resolve these identified concerns. The following indicates general export control processes conducted by ORSP.

- Proposal Stage

- At the time a proposal is setup in Maestro, if a potential agreement involves a non-U.S. person sponsor, ORSP will ensure the “international collaboration” compliance item is marked in Maestro.
- ORSP will conduct RPS on the non-U.S. person sponsor. Should ORSP identify any potential red flags through RPS that are not easily resolvable, the A&M-VICTORIA EO will be notified and a resolution determined.

- Negotiation Stage
    - ORSP will conduct RPS for all sponsors (except for other System members and state or federal agencies) at the agreement setup phase. Detailed ORSP procedures related to RPS hits and recordkeeping are contained in ORSP’s internal operating procedures.
    - ORSP will also complete the A&M-VICTORIA *Export Control Determination Form*. This form will be completed by the ORSP negotiator and is utilized to confirm that the applicable export control-related compliance items are marked on the Maestro compliance module. Detailed ORSP procedures related to the export control determination form are contained in ORSP’s internal operating procedures.
    - Upon notification through the Maestro compliance module, ORSP will resolve export control-related matters. ORSP will work with the involved parties as appropriate and determine what course of action should be taken to address the matter. In many cases, no export control license or other authorization may be necessary. Once concerns are resolved, ORSP will authorize the marked items within the Maestro compliance module.

AGREEMENTS (NON-SPONSORED)

From time-to-time, A&M-VICTORIA may execute non-sponsored agreements—*such as a memorandum of agreement, memorandum of understanding, and independent contractor designations*—with international implications. Such agreements processed through A&M-VICTORIA Finance Procurement will be reviewed by Research and Sponsored Programs for export control-related concerns. RPS will be conducted on all international sponsors. A&M-VICTORIA Finance Procurement and Historically Underutilized Businesses Programs will notify the Research and Sponsored Program by forwarding agreements so RPS and export control assessments can be conducted. Research and Sponsored Programs will return the assessment to A&M-VICTORIA Finance Procurement as notification of the completed process.

FINANCIAL TRANSACTIONS

Export control-related risks within financial transactions are multi-faceted. It is important to establish risk-based procedures to identify export-controlled items or information entering the A&M-VICTORIA inventory, and to identify potential restricted parties involved in the acquisition process. A&M-VICTORIA utilizes a variety of mechanisms to procure goods and services. It is extremely important for ORSP to be informed prior to ITAR-controlled items or information being acquired. RPS is conducted on vendors prior to being set up in the accounting system.

All A&M-VICTORIA employees involved in procurement procedures should consider the following:		
Has the vendor disclosed that an item is controlled? *Such disclosure might be included in the sales documentation, commercial invoice or packaging slip, product specification page, certification issued by the vendor, or in the software license agreement. If A&M-VICTORIA employees identify items or information that are export controlled, Research and Sponsored Programs should be contacted. The Research and Sponsored Programs can discuss the controls and related risks with the asset manager and determine whether such controls necessitate a TCP. Activities related to use of some controlled items or information may require a license for use within* the U.S. when non-U.S. persons are involved.	**Will fabrication, testing, or development be outsourced?** *A&M-VICTORIA employees seeking to outsource fabrication, testing, or development of an item that could be export controlled should request a determination from the Research and Sponsored Programs.*	**Is it known that the item to be procured will be exported?** *A&M-VICTORIA employees should contact Research and Sponsored Programs if they know that an item to be procured will be exported. Research and Sponsored Programs will conduct an analysis on the item, its destination, and end-user/use to determine if a license is needed for the transaction.*

To facilitate a risk-based methodology in identifying and mitigating export control-related risks in the procurement process, the following procedures are implemented for the A&M-VICTORIA business.

- *Vendors Setup in Jaggaer or FAMIS*
  As a shared service unit, TAMU Financial Management Operations (FMO) is responsible for conducting RPS of vendor setups through the Jaggaer System and FAMIS at the time the vendors are established in the accounting system. Any export control concerns are resolved in accordance with TAMU FMO internal procedures.

- *Procurement Identification*
  A&M-VICTORIA utilizes the Jaggaer system for most procurement transactions. Within the Jaggaer System, A&M-VICTORIA Finance has implemented a risk-based methodology for the identification of items that may warrant heightened safeguarding mechanisms from an export control perspective. In the spirit of establishing processes that achieve a high level of compliance while not adding undue burden, ORSP is set up as procurement "approvers" within the Jaggaer system for these risk–based identified categories. This enables ORSP to identify items before they are procured and implement any safeguarding mechanisms necessitated.

INTERNATIONAL TRAVEL

A&M-VICTORIA employees traveling on A&M-VICTORIA business outside the U.S. or when traveling with A&M-VICTORIA property are responsible for complying with export control laws and regulations. Dependent upon unique circumstances, an export control-related license may be necessitated. This analysis is conducted on a case-by-case basis and depends upon many factors, including but not limited to the following: what items or information are taken abroad; what countries are visited; and/or what entities or individuals A&M-VICTORIA employees will interact with. While planning a trip abroad, A&M-VICTORIA employees should review potential export control implications related to their trip, including the "who, what, when, where, and why" of each case. For example, the traveler should think about what items are necessary to take with them while abroad, what the scope of the trip is, whom they will interact with, and the travel destination. Some travel-related activities or destinations may require a license or be prohibited. Generally, most travel to participate in an international conference will not require an export license. For example, 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 generally considered in the public domain. An open gathering is one where members of the general public are eligible to attend, and attendees are permitted to take notes.

KEY DEFINITIONS

ITAR § 120.34 "Public Domain"

Public domain means information which is published and which is generally accessible or available to the public: through sales at newsstands and bookstores; through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; through second class mailing privileges granted by the USG; at libraries open to the public or from which the public can obtain documents; through patents available at any patent office; through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States; through public release in any form after approval by the cognizant USG department or agency; through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific USG access and dissemination controls. University research will not be considered fundamental research if: the University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or the research is funded by the USG and specific access and dissemination controls protecting information resulting from the research are applicable.

EAR § 734.7 "Published"

Published means when "technology" or "software" is not subject to the EAR and has been made available to the public without restriction upon its further dissemination such as through any of the following: subscriptions available without restriction to any individual who desires to obtain or purchase the published information; libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents; unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public; public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the Internet on sites available to the public; or submission of a written composition, manuscript, presentation, computer-readable dataset, formula, imagery, algorithms, or some other representation of knowledge with the intention that such information will be made publicly available if accepted for publication or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, to researchers conducting fundamental research, or to organizers of open conferences or other open gatherings. Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in § 742.15(b) of the EAR. The following remains subject to the EAR: "software" or "technology" for the production of a firearm, or firearm frame or receiver, controlled under ECCN 0A501, that is made available by posting on the internet in an electronic format, such as AMF or G-code, and is ready

	for insertion into a computer numerically controlled machine tool, additive manufacturing equipment, or any other equipment that makes use of the "software" or "technology" to produce the firearm frame or receiver or complete firearm.

A&M-VICTORIA employees traveling with laptops, cell phones, tablets, or other portable electronic devices must ensure there is no controlled information on these devices unless a license has been obtained for the export or other authorization is in place for the case-specific scenario (i.e., level of controls and destination). Dependent on facts, a number of exceptions or general authorizations may apply. For example, an extremely important exception for travel and items or information subject to the EAR includes § 740.9, *Temporary Imports, Exports, Reexports, and Transfers (TMP)*.

Specifically, the "Tools of Trade" exception within the TMP can apply for temporary exports, such as carrying with you laptops, cell phones, and other items or information subject to the EAR to certain countries. The "Tools of Trade" exception is not available for Country Group E:1. Certain conditions regarding effective control must be met for this license exception to be utilized. Generally, so long as the subjected item or information is shipped no more than one month before the traveler's departure from the United States and remains in the individual's effective control while abroad, this exception may apply. Research and Sponsored Programs can assist travelers in determining if this exception or others may apply to each scenario.

EAR § 740.9(a)(1) "Tools of Trade"

Exports, reexports, or transfers (in-country) of commodities and software as tools of trade for use by the exporter or employees of the exporter may be made only to destinations other than Country Group E:1. The tools of trade must remain under the "effective control" of the exporter or the exporter's employee. Eligible items are usual and reasonable kinds and quantities of tools of trade for use in a lawful enterprise or undertaking of the exporter. Tools of trade include, but are not limited to, commodities and software as is necessary to commission or service items, provided that the commodity or software is appropriate for this purpose and that all items to be commissioned or serviced are of foreign origin, or if subject to the EAR, have been lawfully exported, reexported, or transferred. Tools of trade may accompany the individual departing from the United States or may be shipped unaccompanied within one month before the individual's departure from the United States, or at any time after departure. Software used as a tool of trade must be protected against unauthorized access. Examples of security precautions to help prevent unauthorized access include the following:

(i) Use of secure connections, such as Virtual Private Network connections, when accessing IT networks for activities that involve the transmission and use of the software authorized under this license exception;

(ii) Use of password systems on electronic devices that store the software authorized under this license exception; and

(iii) Use of personal firewalls on electronic devices that store the software authorized under this license exception.

EMPLOYMENT

ORSP, in conjunction with Workday Services and the A&M-VICTORIA Human Resources Office, has established a process to address positions with export control implications. Notifications will be sent to the export control office to alert them when there is a change in employment regarding a position that is tied to export controls. These notifications will be investigated to ensure ongoing export control compliance.

SHIPMENTS

All A&M-VICTORIA employees shipping (or hand-carrying) items outside the U.S. (such as equipment, data, materials, and biologics) are responsible for complying with export control laws and regulations. It is imperative to keep in mind that any transmission of goods or technology outside the U.S. via any methodology (email, hand-carry, shipment) might be subject to export control laws and regulations, whether restricted as an item, technology, prohibited end-user, or prohibited end-use. If the item you intend to ship is subject to the ITAR, a license will most likely be required in every case and might even be generally prohibited (i.e., the final destination is to a country designated in ITAR §126.1). Further, if you intend to ship or hand-carry an item to an embargoed location, an assessment by ORSP is vital, as these locations are subject to vast export control-related restrictions. It is important to note that even though an item could be cleared through U.S. Customs, it could still require an export control-related license. A&M-VICTORIA employees should contact ORSP for assistance in product classification and export restriction analysis when in doubt.

To provide a simplistic example, merely sending a package to an international collaborator could result in an export control violation. Additionally, hand-carrying an item in checked luggage and not returning such an item could result in an export control violation. A&M-VICTORIA employees should be aware that a shipping-related export control violation can be severe and result in both institutional or individual fines and or individual imprisonment. A&M-VICTORIA employees should make a concerted effort to contact ORSP for an export restriction analysis prior to shipping anything outside of the U.S. Additionally, every effort should be made to correctly label packages and accurately present the export classification. Regardless of the intent, mislabeling or reporting inaccurate values on the Shippers Export Declaration is also a violation of the law. Further, once an item is cleared for shipment, A&M-VICTORIA might be responsible for further reporting requirements, such as those imposed by the Foreign Trade Division of the Census Bureau, administering the Foreign Trade Regulations (FTR). Generally, if an item is exported without first obtaining the properly licensed authorization from BIS or DDTC, not only would a voluntary disclosure need to be made to either of those entities, but another would need to be made under the FTR as well. If working with a freight-forwarder, A&M-VICTORIA employees should be aware that additional reporting might be required under the FTR for shipments valued greater than $2,500 per the item's Schedule B number and for any licensable shipment and should request proof of such Automated Export System (AES) filing. Thus, international shipments must be classified appropriately, cleared, and appropriate licenses obtained (if necessary) before the transaction occurs. The Research and Sponsored Programs is available to assist you in all export license determinations.

TECHNOLOGY COMMERCIALIZATION

Securing and protecting intellectual property is vital, with export controls compliance procedures contributing to achieving appropriate safeguarding mechanisms. Texas A&M Innovation works closely with the System RSO in developing internal procedures related to export controls compliance and serves as the gateway for disclosure of inventions and commercialization of such inventions. Pursuant to System Regulation 17.01.02, *Evaluation and Protection of Intellectual Property*, A&M-VICTORIA employees are required to promptly disclose to Texas A&M Innovation any intellectual property developed in which the System has an ownership interest under provisions outlined in System Regulation 17.01.01, *Ownership of Intellectual Property and Tangible Research Property*.

TECHNOLOGY CONTROL PLANS

If Research and Sponsored Programs determines that an activity, item, or facility necessitates enhanced protection from an export control perspective, Research and Sponsored Programs will work closely with all involved parties as appropriate to develop and implement a TCP. The Research and Sponsored Programs has developed a TCP template that includes relevant safeguard categories where the activity, item, or facility-specific details will be included. TCP elements generally include:

- compliance commitment statement;
- relevant reasons for control to include jurisdiction and appropriate categories;

- citizenship status, personnel screening measures, and training requirements for all authorized personnel; and

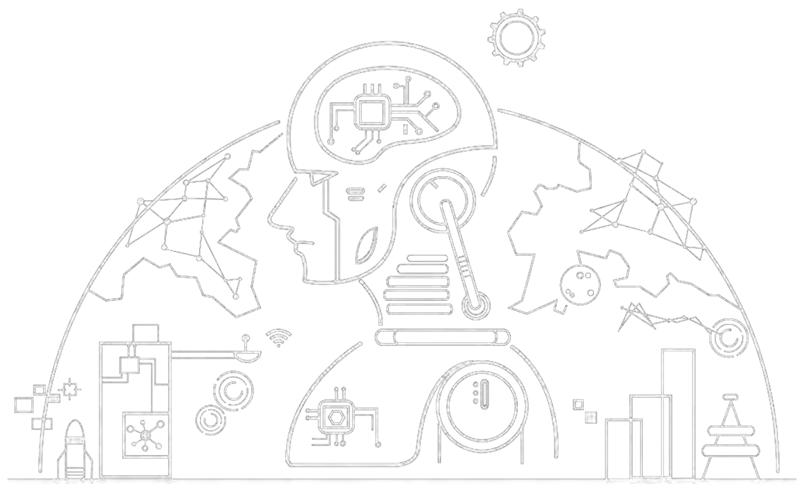
- physical and informational security measures for both duration and termination of the activity, item, or facility.

Examples of security measures are specific to the activity, item, or facility necessitating the TCP. However, the following measures illustrate potential security measures appropriate for a TCP.

- *Laboratory Compartmentalization*—The subjected activity, item, or facility may be limited to secured areas that are physically shielded from access or observation by unauthorized persons. An example might include a laboratory containing ITAR items that has a second area that is secured via swipe–card access, and only authorized U.S. persons are provided swipe-card access to that specific area within the laboratory.

- *Locked Storage*—The subjected activity, item, or facility may be stored within laboratories in storage vessels inclusive of key-controlled access. An example might include a laboratory that is secured via swipe-card access, where ITAR items are additionally secured via a locked cabinet within the secured laboratory.

- *Scheduling*—The subjected activity, item, or facility may be limited to use during specified secure times where unauthorized persons cannot participate. An example might include a laboratory containing ITAR items that is secured via swipe–card access, where the ITAR items are also secured via locked cabinet within the laboratory. The laboratory is utilized for a specified time period for basic fundamental research and use of non-ITAR items by authorized U.S. persons and non-U.S. persons. At other times, when ITAR controlled research is to take place, Non-U.S. persons are not allowed to access the laboratory during that timeframe. The ITAR items are only to be unlocked and utilized during a timeframe when <u>*only*</u> authorized U.S. persons can access the laboratory.



- *Marking*—The subjected activity, item, or facility could be clearly identified and marked as restricted. An example of marking might include clearly identifying a certain item as subject to the ITAR.

- *Information Security*—Electronic devices and networks storing subjected information (including digital communications) will be secured through use of appropriate information security such as, user IDs, password controls, 128-bit or greater encryption, or other approved encryption technology. Virtual private networks (VPNs) should also be utilized.

- *Personnel Identification*—Personnel may be required to provide identification, such as a badge or other card, indicating they have authorization to participate or access a restricted area. An example might include a laboratory containing ITAR items that is secured via swipe-card access, and only authorized U.S. persons are provided swipe–card access to the laboratory. Swipe-card access may be logged.

- *Other Communications*—Communications regarding the subjected activity, item, or facility will be limited to authorized personnel. Such communications cannot occur in the presence of non-authorized personnel. This includes discussions with third-party individuals who are not authorized personnel. If third-party personnel require access to communications regarding the subjected activity, item, or facility, an agreement that identifies the associated export control restrictions shall be executed and any necessary export licenses must be approved and received before providing the third party with the controlled information or communications

GOVERNMENTAL APPLICATIONS & LICENSING

Several federal regulatory entities determine which technology, items, information, goods, and services are subject to their specific jurisdictions and, thus, which items or information may require an export license prior to being exported outside the U.S. or being shared with non–U.S. persons within the U.S. Although many government agencies are involved in export control administration, there are three primary jurisdictions: the Department of State (DDTC), the Department of Commerce (BIS), and the Department of Treasury (OFAC). Prior authorization may be required from any of the federal regulatory entities to export the item or information outside the U.S. or to a non–U.S. person within the U.S. These federal agencies can also provide official determinations regarding appropriate jurisdiction and licensing for authorized exports if necessary. The System RSO serves as the responsible office for A&M-VICTORIA when submitting official commodity jurisdictions, advisory opinions, and licensing documentation to the cognizant federal agency involved. ORSP will work closely with A&M-VICTORIA employees to determine when a license is required and prepare the official determination or licensing package.

TRAINING

Training is imperative as a pillar of an effective export control compliance program. Many resources are available for A&M-VICTORIA employees related to training, whether self-guided online materials or face-to-face training sessions conducted by the Research and Sponsored Programs upon request. Currently, the System provides online training courses available via TrainTraq. Specifically, TrainTraq Course #2111212, Export Controls and Embargo Training, provides a holistic overview and introduction to export control-related compliance. It is important to note that this training is general in nature and not an in-depth analysis of every potential export controls implication related to business conducted at A&M-VICTORIA. Because export controls compliance is multi-faceted and spans almost all business conducted at the A&M-VICTORIA, TrainTraq Course #3001, Information Security Awareness, also includes a brief export control-related component. This training is required annually for all A&M-VICTORIA employees. Additionally, ProCard training delivered via TrainTraq also includes an export controls-related component. This course is required for all Procard holders. At this time, not all A&M-VICTORIA employees are required to complete TrainTraq Course #2111212. However, the following employees are required to do so, once every two years:

- any A&M-VICTORIA employee listed as the responsible individual or a participant on an A&M-VICTORIA TCP;
- any A&M-VICTORIA employee at the discretion of their supervisor.

RECORDKEEPING

Applicable federal regulations stipulate the timeframe necessitated for keeping records related to export control assessments and transactions. For example, records are required to be maintained for the longer of:

- the record retention period required by the applicable regulations (i.e., 15 C.F.R Part 762 of the EAR; 22 C.F.R. Parts 122.5, 123.22, and 123.26 of the ITAR; and 31 C.F.R. Part 501.601 of the OFAC; or

- the period required for the retention of records as set forth in A&M System policies and regulations, A&M-VICTORIA rules and procedures, and the System records and retention schedule.

All export control compliance analysis A&M-VICTORIA records will be maintained and managed centrally by ORSP and stored in the file storage location. Examples of such records include any notes, correspondence (including email and official memoranda), financial records, restricted party screenings, classification determinations, and any other information related to export-controlled or potentially export-controlled activities analyzed by ORSP for A&M-VICTORIA.

INTERNAL MONITORING

Internal monitoring is necessary to proactively mitigate risk within the A&M-VICTORIA export controls compliance program. Unlike an external audit, internal monitoring is conducted by an audit group within the university system at intervals dictated by the Research and Sponsored Programs. The purpose is to help identify weaknesses in the export control processes from an unbiased, objective perspective and to provide criticism, suggestions, and input based on internal findings. Another internal monitoring mechanism implemented to mitigate risk is a risk assessment tool. This tool is used to conduct a self-analysis to identify gaps in compliance and help address them. These areas of vulnerability, in turn, are measured at different risk levels, which are prioritized and addressed accordingly.

POSSIBLE VIOLATIONS & DISCIPLINARY ACTIONS

As a foundational pillar of an effective export control compliance program, known or suspected violations shall be investigated, corrected appropriately, and reported. Penalties for non-compliance can be both institutional or individual and civil or criminal, potentially constituting significant fines and loss of export privileges. Individuals can also be subject to incarceration. Violations of the EAR can include criminal fines in excess of $1M per violation, imprisonment, or both. Illegally exported items could be seized or forfeited as well. Regarding OFAC, penalties generally vary by specific sanctions programs, with possible fines and or imprisonment. Violations of the ITAR for criminal convictions can result in imprisonment and fines in excess of $1M per fine for each violation. For civil violations of the ITAR, fines can be levied, and export privileges can be denied. A&M-VICTORIA employees may be subject to disciplinary action up to and including termination per System policies, regulations, rules, and procedures.

If an A&M-VICTORIA employee knows of a suspected export control violation or believes a violation might occur, the employee is responsible for reporting such a violation or potential violation. A&M-VICTORIA employees can report such occurrences through any of the following methodologies:

- to the A&M-VICTORIA EO;
- via the A&M System EthicsPoint Hotline.

Reported potential or actual violations will be investigated to the extent deemed necessary by Research and Sponsored Programs in consultation with System RSO and System OGC. The A&M-VICTORIA EO may declare business activities or transactions under investigation in “export control hold” status until the investigation is completed. If a notification to the appropriate federal regulatory agency is necessitated, the System RSO will work closely with System OGC.

6.0 RELATED STATUTES, POLICIES, OR REQUIREMENTS

FEDERAL

Department of State
Directorate of Defense Trade Controls

International Traffic in Arms Regulations
22 CFR Parts 120-130

United States Munitions List
22 CFR Part 121

Department of Commerce
Bureau of Industry and Security

Export Administration Regulations
15 CFR Parts 730-774

Commerce Control List
15 CFR Part 774

Department of Treasury
Office of Foreign Assets Control

31 CFR Parts 500-599

Arms Export Controls Act | 22 USC 2778

International Emergency Economic Powers Act | 50 USC 1701

National Defense Authorization Act for 2019 | Public Law No: 115-232

LOCAL

System Policy 15.02, *Export Controls Program Management*

15.02.99.J1 Export Control Program Management | Texas A&M University-Victoria

University/Agency Technology Control Plan (Coming Soon)

University/Agency Export Control Determination Form (Coming Soon)

7.0 CONTACT INFORMATION

Research and Sponsored Programs

EXPORT CONTROL

University West Suite 272
Research and Sponsored Programs | Texas A&M University-Victoria
| 361-570-4374 | RSP@A&M-Victoria.edu