POLICY ON EXPORT CONTROLS

DIVISION: **Research and Economic Development (RED)/Office of Research Compliance (ORC)**

TITLE: **Policy on Export Controls**

DATE: **October 27, 2023**

Table of Contents

OVERVIEW OF EXPORT CONTROLS

This Export Compliance Manual outlines the policies and procedures to be followed when implementing AAMU's Export Compliance Program (ECP). The ECP policy applies to all AAMU investigators, faculty, staff, visiting scientists, postdoctoral fellows, students, scholars, and other persons working at or for AAMU or related entities. Thus, AAMU's ECP is a university-wide program established to ensure that AAMU (and related entities, including AAMU-RISE Foundation) is fully compliant with all applicable U.S. export control laws and regulations. Non-compliance with U.S. export control regulations could result in criminal, civil, or administrative penalties against AAMU as an entity and the individual faculty or staff member who commits the violation. AAMU's export compliance program has the challenging task of maximizing the benefits of AAMU's international relationships with both universities and students while ensuring compliance with all appropriate U.S. export control laws and regulations.

U.S. export control regulations are written to protect U.S. technology, specifically for defense items that have both commercial and military applications and exports to sanctioned persons and destinations. U.S. national security, economic interests, and foreign policy shape the U.S. export control regime and provide the rationale for when technology requires an export license for export. The export laws and regulations also aim to achieve various objectives, such as preventing the proliferation of weapons of mass destruction, advancing the U.S. economic interests at home and abroad, aiding regional stability, implementing anti-terrorism and crime controls, and protecting human rights. Additionally, an export is not only the physical product or technology crossing an international border; the export control regulatory agencies also consider providing this same technology or product to a foreign national inside the United States as an export. For example, suppose military space technology was shown to a student from Iran on the AAMU campus. In that case, U.S. regulatory agencies consider that this technology has now been exported to Iran, a U.S. embargoed country, violating export control regulations.

These regulatory controls generally restrict the export of products and services based on the product type and the export destination. In defense and high-technology sectors, the U.S. Government tightly regulates the export of equipment and components (called defense articles) and technology. Technology includes technical data, such as blueprints and manuals, design services (including the transfer of "knowledge"), and training, also referred to as a defense service. U.S. laws assert jurisdiction over U.S.-origin equipment and technology even after it is exported (i.e., restricting the re-export or re-transfer to third parties). In addition to general export licensing, the United States maintains economic embargoes against several countries whose governments consistently violate human rights or act in support of global terrorism. Such embargoes bar most transactions by U.S. persons with these countries. Finally, the U.S. Government maintains lists of Specially Designated Nationals or persons and entities that are banned from conducting export business because of previous activities. Three principal agencies regulate exports from the United States (Table 1).

Table 1. Export Control Regulations

Governing Agency	Mechanism	Covers
U.S. Department of State Directorate of Defense Trade Controls (DDTC)	International Traffic in Arms Regulations (ITAR)	Items designed for military use, defense services
U.S. Department of Commerce (DoC) Bureau of Industry and Security (BIS)	Export Administration Regulations (EAR)	Dual use Technology
U.S. Department of the Treasury	Office of Foreign Assets Control (OFAC)	Sanctioned/embargoed/specially designated countries/entities

GENERAL AAMU POLICY ON EXPORT CONTROL COMPLIANCE

While AAMU endorses the principles of freedom of inquiry and open knowledge exchange, AAMU also recognizes and respects its obligation to comply with U.S. export control regulations. The export of certain technologies, software, and hardware is regulated and controlled by Federal law for national security, foreign policy, weapons of mass destruction prevention, and competitive trade reasons. AAMU and all its employees are required to comply with the laws and implementing regulations issued by the Department of State through its International Traffic in Arms Regulations (ITAR), the Department of Commerce through its Export Administration Regulations (EAR), and the Department of the Treasury, through its Office of Foreign Asset Controls (OFAC).

While most research conducted by researchers at AAMU is excluded from these regulations under the Fundamental Research Exclusion, university research involving specified technologies controlled under the EAR and/or ITAR or transactions and exchanges with designated countries, individuals, and entities may require AAMU to obtain prior approval from the appropriate agency before allowing foreign nationals to participate in controlled research, collaborate with a foreign company and/or share research, verbally or in writing, with persons who are not United States citizens or permanent residents. The consequences of violating these regulations can be severe, ranging from loss of research contracts and exporting privileges to monetary penalties and jail time for the individual violating these regulations. Institutional consequences may range from fines to revocation of institutional export privileges to institutional debarment from receipt of federal research funds, which would affect a majority of AAMU's research grants and contracts.

The export control regulations affect research conducted on campus and travel and shipping items outside the U.S. Simply traveling to certain sanctioned countries could require a license from OFAC. OFAC sanctions prohibit transactions and exchange of goods and services in certain countries and with designated persons and entities. Multiple lists of denied individuals and parties are maintained and enforced by federal agencies, including the Departments of State, Commerce, and Treasury. Shipping items outside the U.S. and taking controlled items on a flight, even if shipping or traveling in the conduct of research, could require a license from these agencies.

Export Controls and University Research
U.S. national security and economic interests depend heavily on technological innovation and advantage. Many of the nation's leading-edge technologies, including defense-related technologies, are being invented by U.S. and foreign national students and scholars in U.S. university research and university-affiliated laboratories. U.S. policymakers recognize that international students and researchers have contributed substantially to U.S. research efforts. Still, the potential transfer of controlled defense or dual-use technologies to their home countries could have significant consequences for U.S. national interests. The U.S. export control agencies place the onus on universities to understand and comply with the regulations.

AAMU researchers and administrators need to be aware that these laws may apply to any research, whether sponsored or not. However, it also is important to understand the extent to which the regulations do not affect normal university activities. As noted before, the policy applies to all AAMU investigators, faculty, staff, visiting scientists, postdoctoral fellows, students, scholars, and other persons working at or for AAMU or related entities (e.g., AAMU-RISE Foundation). The policy sets forth the basic responsibilities that all such persons must meet in conducting their research, teaching, consultancy, or other activities at or on behalf of the University. The primary individuals and entities and their responsibilities are described below.

ROLES AND RESPONSIBILITIES

Office of Research Compliance (ORC)
The ORC has the requisite knowledge to support export transactions for export-controlled products and technology. Any export of controlled technology or suspected export of controlled technology must be arranged through the ORC to acquire the necessary export licenses or apply the available exemptions that may be applicable. The Office of Research Compliance and the AAMU Office of General Counsel will act as the liaison to all federal agencies involved in export control, primarily the Department of State, the Department of Commerce, and the Department of Treasury.

If there is ever any doubt or open questions concerning the export of technology or products, ORC is available for consultation and should be incorporated early on in any export process, including the involvement of international students and faculty in research projects.

Export Control Manager (ECM)
The University's Export Control Manager (ECM) is responsible for export control oversight, including developing and implementing procedures to promote the University's ongoing compliance with export control laws and developing training and education for faculty and staff. The ECM is an Empowered Official and Export Control Advisory Committee Chair. The ECM duties are to:
- Provide education and guidance to faculty and staff
- Promote a culture of export control awareness and compliance
- Conduct export control reviews
- Oversee restricted party screening processes
- Implement Technology Control Plans
- Submit license applications, classification requests, and advisory opinions and act as the main point of contact for official communications

- Review H1-B Visa applications for I-129 export control certifications
- Coordinate with other University entities to facilitate export control compliance

Faculty/ Principal Investigators and Directors
Faculty, Principal Investigators (PI), and Directors will have primary responsibility for assuring that their research and other activities comply with export control regulations. Faculty/PI/Director responsibilities are to:
- Understand how the Export Control Laws may affect their activities and when to call the University Export Control Manager (ECM) for assistance.
- Assure that they and their staff are informed about export controls and the resources available to enable compliance.
- Establish and maintain standards of export control compliance for locations and personnel under their direction.
- Cooperate with the ECM to evaluate and manage potential export control issues such as shipping, travel, and deemed exports.
- Manage access by unlicensed foreign persons to any identified controlled technology or technical data in areas under their supervision that do not qualify for an exclusion to export control regulations. This may require compliance with a *Technology Control Plan* and/or working with the ECM to obtain an export control license.
- Coordinate and cooperate with the ECM to obtain necessary export control licenses from the appropriate federal agency. If that license is granted with provisos, the PI must ensure that the conditions of the license are met and maintained.
- Contact the ECM for restricted party screening of shipping destinations, foreign travel destinations, and potential collaborators and visitors as necessary.
- Complete the required export control training on an annual basis.

Senior Official
The Vice President for Research and Economic Development (VP-RED) is the senior official representing AAMU to Federal Agencies with export control authority.

Empowered Officials
Empowered officials represent AAMU in official export control matters such as registrations, licensing, commodity jurisdiction and classification requests, and voluntary self-disclosures. They have the authority to sign paperwork binding the University in proceedings with any agency with export control oversight. AAMU's empowered officials are the Export Control Manager, the Research Compliance Officer, and the AAMU-RISE Executive Director.

Export Control Advisory Committee (ECAC)
The Export Control Advisory Committee (ECAC) provides guidance and makes recommendations to University Officials and the Export Control Manager on export control policies and procedures. Members of the ECAC provide input on education and training, compliance programs and policy, technology and tool needs, and provide subject matter expertise in their areas of responsibility. They assist with developing export control compliance action plans and periodic program reviews and facilitate communication throughout the University community about the importance of export control compliance. The Export Control Manager chairs the ECAC. Membership of the ECAC

includes representatives of the following cooperating entities: Office of Sponsored Programs, Research, Innovation, Science and Engineering Foundation, Environmental Health and Safety, Community College Relationship and Global Initiatives, Purchasing Office, Information Technology, Human Resources, and the Office of General Counsel.

RESPONSIBILITIES OF THE COOPERATING ENTITIES

Many units of the University coordinate with the Export Control Manager (ECM), including the following offices, which are represented on the Export Controls Advisory Committee:

Office of Sponsored Programs (OSP)
The Office of Sponsored Programs (OSP) supports AAMU faculty and administrative personnel in all aspects of their work associated with the proposal and acceptance of research projects with federal, industry, and private sources. The OSP grant team will work with the ECM to identify proposed and funded projects with potential export control issues.

Research, Innovation, Science and Engineering (RISE) Foundation
The AAMU-RISE Foundation facilitates the timely execution of federal contracts, industry-supported research agreements, and other research-related agreements. The Office will work closely with the ECM to identify and resolve potential export control concerns in research agreements.

Environmental Health and Safety (EH&S)
Environmental Health and Safety (EH&S) provides oversight and consulting in all safety, health, and environmental compliance areas. It includes the Institutional Biological and Chemical Safety Committee (IBC). The IBC oversees research involving recombinant DNA, infectious or potentially infectious agents, and/or hazardous chemicals. It works closely with the ECM to identify potential concerns for biological and chemical export control.

Community College Relations and Global Initiatives
The Office of Community College Relations and **Global Initiatives (GI)** provides resources and support services to international students and scholars, including integration into the U.S., language assistance, and expertise on immigration and visa matters. The Office will work closely with the ECM on the I-129 certification process for H-1B Visas and alerts the ECM to matters of export control concern regarding international students, postdoctoral fellows, and visiting scholars.

Purchasing Office
The Purchasing Office conducts restricted party screening on new vendors and many foreign transactions. IT will work with the ECM on export control issues related to information technology.

Information Technology (IT)
The AAMU Information Technology offices oversee information technology services and security and will work with the ECM on export control issues related to information technology.

Human Resources (HR)
Human Resources (HR) manages recruitment, training and development, compensation and benefits, and employee relations for employees of the University. HR will work with the ECM when export control issues arise regarding foreign national employees.

Office of General Counsel (OGC)
The Office of General Counsel (OGC) provides ad hoc representation and counsel on a broad range of legal issues affecting the University. The OGC will work with the ECM on legal aspects of export control matters. The OGC does not have an official Export Control Advisory Committee representative but gives counsel upon request.

PROCESSES AND PROCEDURES

Restricted Party Screening
"Restricted Party Screening" (RPS) refers to the screening of individuals and entities against restricted party lists and country sanctions. Restricted party screening is conducted by consulting the government Consolidated Screening List. Authorized personnel from relevant university offices can conduct RPS after training by the Export Control Manager (ECM.) The ECM administers the screening program.

Table 2. Restricted Party Screening Processes.

Who is screened?	What Office performs the screening?
Visa applicants sponsored by the University	Export Control Manager (H-1B), Community College Relations and Global Initiatives (other)
New vendors; foreign financial transactions	Purchasing Office
Foreign parties to research contracts and service agreements, foreign sub-awards	RISE, Office of Sponsored Programs, Export Control Manager
Foreign parties to Material Transfer and Licensing Agreements	Environmental Health and Safety (biological and chemical), RISE, Export Control Manager
Foreign recipients of tangible exports*	Environmental Health and Safety (biological and chemical), Export Control Manager (other)
Personnel authorized in a Technology Control	Export Control Manager and RISE

Principal Investigators are responsible for contacting the ECM for restricted party screening of international shipping destinations, travel destinations, and foreign visitors (if visitors are not being otherwise processed through the Office of Community College Relations and Global Initiatives).

Export Control Review
Principal Investigators (PI) and department personnel may contact the Export Control Manager (ECM) and request an export control review at any time. The ECM may also select laboratories and departments for review based on the type of research conducted or the technology being used. The

ECM performs export control reviews. The ECM will, in consultation with the Principal Investigator or staff member, evaluate the following questions:

1. Does the research fall under the Fundamental Research Exclusion?
2. Is the technology or technical data subject to export control regulations?
3. If yes, what is the technology or technical data classification under the EAR or ITAR?
4. Do individuals who will access the technology, technical data, or the destination of said technology, if a physical export, require an export license under the EAR or ITAR?
5. Is a management plan (Technology Control Plan; TCP) necessary to protect access to the technology or technical information? If so, the ECM will develop and implement the TCP in consultation with the PI.
6. Are any individuals or entities that will receive or have access to the items restricted parties? If so, the ECM will conduct restricted party screening.
7. Are any of the countries involved sanctioned or embargoed? ([Sanctions Programs and Country Information | U.S. Department of the Treasury](#).

The following circumstances may also trigger export control reviews:

(a) Sponsored Research: Export control review may be triggered when the institution submits a proposal, receives an award, or negotiates a contract. Staff in the Office of Sponsored Programs (OSP) and RISE watch for the following red flags which indicate possible export control issues:
- Restrictions on publication or dissemination of research results
- References to U.S. export control regulations (beyond a statement of general compliance)
- Restrictions on participation or access
- Assertions that the sponsor will provide proprietary information
- Military application of results with no "civil" or "dual" use
- Involvement of foreign military
- Involvement of foreign sponsors

Projects which are flagged are referred to the Export Control Manager (ECM) for review. The ECM (or RISE Executive Director) reviews the project for specific export control issues and works with the OSP grant manager and the Principal Investigator (PI) to negotiate acceptable export control terms and conditions with the sponsor. If the export control issues cannot be eliminated, the ECM (or RISE Executive Director) will work with the PI to implement a Technology Control Plan or apply for a license to ensure compliance with export control regulations.

The vast majority of research conducted at AAMU is fundamental research. Fundamental research projects will be reviewed if one of the following occurs:
- There is an identified need to export technology or technical data overseas.
- Instruments and individuals involved in the conduct of the research meet criteria that trigger the need for a deemed export license (e.g., ITAR).
- The sponsor indicates that the information provided to the University is proprietary and export controlled.

(b) ***Material Transfer Agreements and Licensing Agreements***: Material transfer agreements (MTA) and licensing agreements involving foreign entities are sent to the ECM for review and restricted party screening.

(c) ***H1-B Visa Applicants***: Export control reviews will be triggered when the University sponsors an international student or scholar on an H1-B visa. A preliminary export control questionnaire (see Appendix V) is filled out by the scholar's supervisor and is reviewed by the Export Control Manager (ECM). The ECM follows up with the supervisor if necessary and recommends to the Office of Global Initiatives (**OGI**) whether an export control license is anticipated to be needed for the foreign national's activities on campus. The OGI then uses this recommendation to complete the I –129 form. OGI may also request export control reviews for individuals applying for other classes of visas, for example, a visiting J-1 scholar from a sanctioned country. OGI conducts restricted party screening on applicants for all Visa categories. Potential matches go to the ECM for verification. The ECM performs the restricted party screening on H-1B visa applicants and other visa applicants for which an export control review is conducted.

(d) ***Shipping***: University personnel are responsible for contacting the ECM before shipping items overseas. The ECM will conduct a review to determine the export status of the item, whether a license is needed, or whether a license exception is available. The ECM also conducts restricted party screening on the shipping destination and recipient. In biological and chemical export cases, export control review and restricted party screening are conducted by an authorized individual from the Office of Environmental Health and Safety and/ or the ECM. The ECM reviews potential restricted party matches.

(e) ***Purchases:*** Purchasing Office alerts the ECM if indications that an item is export controlled are identified. Export control training programs provided to faculty and staff by the ECM emphasize red flags to look for when purchasing technology that indicates an item is export controlled. The University's standard vendor contract requires vendors to notify the ECM and receive written authorization of acceptance before delivering any ITAR-controlled items to campus (see Appendix VI). If the ECM is notified of an ITAR purchase, a review will be conducted to ensure that access controls are in place before the item's delivery to campus.

(f) ***Additional Reviews***: The Export Control Manager (ECM) may review selected laboratories or Departments at any time based on their activities or technology. In general, the ECM will meet with an appropriate staff member who is knowledgeable about the technology in use in that area. The ECM will evaluate potential export control issues, and if indicated, a plan will be developed for either license submission or implementation of a Technology Control Plan.

PROTECTING CONTROLLED TECHNOLOGY FROM UNAUTHORIZED ACCESS

Technology Control Plans (TCP)

In cases where it is determined that export-controlled technology or technical information must be protected from unauthorized foreign national access, a Technology Control Plan (TCP) is developed by the Export Control Manager (ECM) in consultation with the Principal Investigator (PI). A TCP is a formal document outlining the procedures used to protect access to controlled technology or technical information. The TCP typically includes

- A statement of commitment to export control compliance by the University;
- Identification of the primary responsible parties;
- Identification and description of the project;
- Identification of the items or technologies and the applicable classification and controls;
- A physical security plan;
- An information security plan; and
- Names and nationalities of all personnel granted access to the item/information.

TCPs must be read and signed by all personnel with authorized access to the controlled technology or technical data. An additional briefing on export controls, including a statement of understanding and commitment, must be read and signed by authorized personnel. Before implementation, the ECM conducts restricted party screening on all personnel included on the TCP. It is the responsibility of the Principal Investigator (PI) and the personnel listed on the TCP to ensure that the conditions of the TCP are followed and to notify the ECM of any changes (locations, protocols, personnel, materials). The ECM must approve protocol changes. The ECM conducts periodic reviews (approximately yearly) of all TCPs. Records related to TCPs will be maintained by the ECM for five years after the TCP is closed out. A TCP and briefing template may be found in Appendix VII of this manual.

Licensing

Export licenses may be required for physical exports, deemed exports, or transactions with restricted entities or embargoed countries. In the case of deemed exports, licenses are specific to foreign nationals, and each foreign national requires a separate license. For example, if there is one ITAR-controlled item in a laboratory and there are four foreign national graduate students in that laboratory who need access to that item, four separate export control licenses will be necessary, one for each foreign national.

1. To determine if a license is required, the following information must be provided by the requestor to the Export Control Manager (ECM):
    - Technology description (Manufacturer, make, model, and purpose in layperson's terms).
    - This will facilitate the classification of the technology by the ECM.
    - Destination
        o Country represented
        o Institution
        o End-User (full name)
        o End-use.

2. License applications are submitted on behalf of the University by the Export Control Manager or other empowered officials.

3. The government agency grants a license to the University; however, the Principal Investigator (PI) is responsible for ensuring that any license provisions are followed.
4. The PI must maintain documentation (e.g., shipping records), and a copy must be submitted to the ECM.

Records and Record Retention
Records will be maintained consistently with applicable law and following plans developed by the college, departments, and other units that hold University Records.

Training
Presentation on the basics of export controls training is available through **CITI online modules**. The ECM conducts additional training annually at faculty and staff meetings across the University to ensure that employees or students engaged in an export-controlled project receive the appropriate instruction. The ECM will conduct training sessions with any group upon request and often meets one-on-one with investigators.

Audits
The Office of Research Compliance verifies that effective compliance occurs in all university activities governed by federal laws and regulations or by University policy. University audits of internal compliance programs are generally conducted every three to five years.

Detecting and Reporting Violations
To maintain AAMU's export compliance program and ensure consistent adherence to
U.S. export laws, the ECM may conduct internal reviews of TCPs and certain projects. The reviews aim to identify possible violations and deficiencies in training, procedures, etc., that can be rectified.

It is the policy of AAMU to voluntarily self-disclose violations as required. Any individual who suspects that an export control violation has occurred should notify the University through one of these channels:
- Contact the Export Control Manager directly at research.compliance@aamu.edu
- Call the University Compliance hotline at 256-372-5729

Individuals may report anonymously. The Export Control Manager will investigate the suspected violation by gathering information and will review the case in conjunction with the Office of General Counsel and the Office of Research Compliance to determine if a violation has occurred and if subsequent self-disclosure to a government agency is needed. If it is determined that a self-disclosure is required, the disclosure will be handled and submitted by the Export Control Manager or other empowered officials.

APPENDAGE

Appendix I: Department of State International Traffic in Arms Regulations (ITAR).

Appendix II: Department of Commerce Export Administration Regulations (EAR).

Appendix III: Department of Treasury Office of Foreign Assets Control (OFAC).

Appendix IV: Penalties.

Appendix V: Export Control Questionnaire.

Appendix VI: ITAR Language in AAMU Purchase Terms and Conditions.

Appendix VII: Technology Control Plan and Briefing.

Department of State
International Traffic in Arms Regulations

Regulatory Authority and Scope

The Arms Export Control Act (AECA)[1] grants authority to the president of the U.S. to regulate the export and import of defense articles and services. The President has delegated this responsibility to the Secretary of State.[2] The Department of State Directorate of Defense Trade Controls (DDTC) administers these controls through the International Traffic in Arms Regulations (ITAR)[3] and lists the designated articles on the United States Munitions List (UMSL).[4]

Items Controlled under the ITAR
The USML includes defense articles and associated technical data. It is important to note that these items were designed for military purposes and that they are controlled for export regardless of how they are being used on campus. ITAR controlled items require licenses form the DDTC for physical export of for technology release to foreign nationals within the U.S. (deemed export). The license requirement applies to foreign nationals from all countries, and includes students and postdoctoral fellows. No licenses are available for nationals from the People's Republic of China.

USML Categories

The USML defines twenty one classes of defense articles[5]. Below is a list of category headings. The full regulations including the USML can be accessed at

 https://www.govinfo.gov/content/pkg/CFR-2016-title22-vol1/xml/CFR-2016-title22-vol1-chapI-subchapM.xml

or for a slightly more user friendly version, see

https://www.law.cornell.edu/cfr/text/22/chapter-I/subchapter-M

Category I-Firearms, Close Assault Weapons and Combat Shotguns
Category II-Guns and Armament
Category III-Ammunition/Ordnance
Category IV-Launch Vehicles, Guided & Ballistic Missiles, Rockets, Torpedoes, Bombs and Mines
Category V-Explosives and Energetic Materials, Propellants, Incendiary Agents and 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-Protective Personnel Equipment and Shelters
Category XI-Military Electronics
Category XII-Fire Control, Range Finder, Optical and Guidance and Control Equipment
Category XIII-Materials and Miscellaneous Articles

---

[1] 22 USC 2778, Chapter 39
[2] Executive order 11958
[3] 22 CFR §§ 120-130
[4] ITAR §121
[5] 22 CFR §121

Category XIV-Toxicological Agents, including Chemical and Biological Agents, Associated Equipment
Category XV-Spacecraft Systems and Associated Equipment
Category XVI-Nuclear Weapons Design and Testing Related Items
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

Exporting Under the ITAR

Transferring defense articles outside of the U.S., disclosing or transferring technical data to foreign nationals within the U.S., or performing a defense service for the benefit of a foreign person within the U.S. or abroad constitute an export under the ITAR[6]. In cases where technology is released to a foreign national within the U.S., the export is deemed to occur to *all* countries that foreign national has held or holds citizenship or permanent residency.

If there is doubt as to whether an item is controlled under the ITAR, an empowered official can submit a written "Commodity Jurisdiction" request to the DDTC, which will determine which regulations apply (EAR or ITAR).   U.S. entities wishing to export ITAR controlled articles must be registered with the DDTC[7]. Registration is required in order to apply for ITAR export licenses.

The ITAR also contains country-based prohibitions[8], prohibiting exports to countries under embargos. For example China is under a U.S. arms embargo with a current policy of denial for license requests. It is not possible to obtain a license for an ITAR export or deemed export to China. These embargoes are subject to change and can be checked at
https://www.pmddtc.state.gov/embargoed_countries/?id=ddtc_public_portal_country_landing/.
Also see ITAR §126.1 .

Important ITAR Definitions

Defense Article[9] refers to anything listed on the U.S. Munitions List and related technical data. It may also include articles that provide the equivalent performance capabilities of a defense article on the USML.   It does not include basic marketing information on function or purpose or general system descriptions.

Defense Service[10] means the furnishing of assistance (including training) to foreign persons, whether in the U.S. or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles. It also includes the furnishing to foreign persons of ITAR controlled technical data and military training of foreign units and forces, regular and irregular, including formal or informal instruction 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.

---

[6] 22 CFR §120.17
[7] 22 CFR §122.1
[8] 22 CFR §126.1
[9] 22 CFR §120.3
[10] 22 CFR §120.9

Release[11] (a) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person or (b) oral or written exchanges with foreign persons of technical data in the U.S. or abroad.

Technical Data[12] refers to information other than software[13] which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation. Technical data also includes classified information relating to defense articles or services or to 600 series items on the Commerce Control List, information covered by an invention secrecy order, or software directly related to defense articles.

---

[11] 22 CFR §120.50
[12] 22 CFR §120.10
[13] as defined in CFR § 120.10(a)(4)

**Department of Commerce
Export Administration Regulations (EAR)**

Regulatory Authority and Scope

The U.S. Department of Commerce Bureau of Industry and Security administers the EAR under the Export Administration Act (EAA) of 1979[14], as amended. This act has lapsed but its authority has been extended by Presidential Executive Orders under the International Emergency Economic Powers Act (IEEPA)[15]. The EAR controls "dual use" items, software, and technology. These are items that have civilian uses (as well as possible military uses in some cases) and may be controlled for reasons other than national security.

Items Controlled under the EAR

The EAR is traditionally described as controlling "dual use" items which have both military or strategic and civilian uses. However, the EAR also controls items with strictly civilian uses, and some military items which have been transferred from the ITAR as part of export control reforms. Generally all items of U.S. origin or located in the U.S. are controlled by the EAR unless under the jurisdiction of another regulatory agency. Items specifically controlled by the Departments of State (ITAR), Treasury, Energy, Nuclear Regulatory commission and the Patent and Trademark Office are excluded from the scope of the EAR[16].

The [Commerce Control List (CCL)](#)[17] identifies items subject to specific EAR control and license requirements. It is divided into 9 categories. Items are given an Export Control Classification Number (ECCN) composed of the category number, a letter, and three additional numbers (for example 1C350).

Commerce Control List Categories

• Category 0 Nuclear Materials, Facilities and Miscellaneous
• Category 1 Materials, Chemicals, Microorganisms, and Toxins
• Category 2 Materials Processing
• Category 3 Electronics
• Category 4 Computers
• Category 5 Part 1: Telecommunications Part 2: Information Security
• Category 6 Lasers and Sensors
• Category 7 Navigation and Avionics
• Category 8 Marine
• Category 9 Propulsion Systems, Space Vehicles, and Related

The second character, a letter, indicates the type of item controlled (A-E). Each CCL Category is subdivided into five (5) Groups:

(A) Equipment, assemblies, and components
(B) Test, inspection and production equipment

---

[14] 15 CFR Chapter VII, Subchapter C
[15] PL 95-223; 50 USC 1701 *et seq.*
[16] 15 CFR §734.3(b)(1)
[17] 15 CFR §774 Supplement 1

(C) Materials
(D) Software
(E) Technology

For example, ECCN 1C350 indicates that it is in Category 1, "Materials, Chemicals, Microorganisms, and Toxins", and the item type is C, "Materials".

Each ECCN has unique licensing requirements. Items that are subject to the EAR but that do not have specific licensing requirements are categorized as EAR99. EAR99 items have very few controls and are mainly of concern when dealing with sanctioned or embargoed countries, restricted entities, or a prohibited end-use.   In the event of an incorrect classification, the exporter is liable for resulting violations.

Exporting under the EAR
Similar to the ITAR, the EAR defines an export as shipment or transfer of items out of the U.S. or the release of technology or source code to a foreign national within the U.S.[18] Release of technical data or source code to a foreign national within the U.S. is considered a deemed export. In contrast to the ITAR, under the EAR a deemed export is considered to be an export to only the *most recent* country of citizenship or permanent residency of the foreign national.

Important EAR Definitions[19]

Development
Related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts.

Production
All production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

Re-export
Shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner. For full definition see 15 CFR § 734.14.

Release[20]
Visual or other inspection by a foreign person of items that reveals" technology" or source code subject to the EAR to a foreign person: or oral or written exchanges with a foreign person of "technology" or source code in the U.S. or abroad. Any act causing the "release" of "technology" or software through use of "access information" or to yourself or another person requires an authorization to the same extent an authorization would be required to export or re-export such "technology" or software to that person.

Required
As applied to "technology" or "software", refers to only that portion of "technology" or "software" which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.

---

[18] 15 CFR § 734.2
[19] 15 CFR § 772.1
[20] 15 CFR § 734.15

Technical assistance
May take forms such as instruction, skills, training, working knowledge, consulting services. 'Technical assistance' may involve transfer of 'technical data'.

Technical data
May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read only memories.

Technology
Information necessary for the "development," "production," "use," (operation, installation, maintenance, repair, overhaul, or refurbishing or other terms specified in ECCNs on the CCL that control "technology" of an item). "Technology" not elsewhere specified on the CCL is designated as EAR99, unless the "technology" is subject to the exclusive jurisdiction of another U.S. Government agency or is otherwise not subject to the EAR. "Technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection.

Use
Operation, installation, maintenance , repair, overhaul and refurbishing.

Determining License Requirements under the EAR

Once the ECCN has been determined the license requirements can be determined. The reasons for control affect which country destinations will need licenses. More than one reason may apply. These reasons include:

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

For details and the complete list see 15 CFR §742. The most common reasons for controls are AT, NP and NS. After the controls are determined (for example AT1), the user must refer to the Country Control Chart[21]. If the country in question has an "X" in the appropriate column (e.g. AT1) then an export to that country will require a license from the Department of Commerce Bureau of Industry and Security (BIS).

---

[21] 15 CFR §738 Supp 1

The ECCN listing will give detailed information on reasons for control and possible license exceptions that are available. University personnel wishing to determine technology classification and license requirements should contact the Export Control Manager for an export control review.

<u>License Exceptions</u>

The EAR contains a number of exceptions that may be used in some cases. The details of each case as well as the notes on applicable license exceptions listed in the ECCN must be reviewed to ensure correct interpretation and use of license exceptions. Descriptions of all license exceptions can be found at 15 CFR § 740.

Two exceptions which can at times be used for temporary exports are "BAG" and "TMP". U.S. persons or authorized foreign persons may take personal devices out of the U.S. under the "BAG"[22] exception and University owned devices under the "TMP"[23] exception, ***if***:

- The device will be returned to the U.S. within 12 months
- The device and technology will remain in the traveler's effective control throughout the trip (in physical possession or in a secured space e.g., hotel safe)
- Controlled technology is not released or shared while overseas
- Traveler takes responsibility for preventing inadvertent releases. Use secure connections, a password to protect technical data, and firewalls.
- The device does not contain non-mass-market encryption applications or software
- The device does not contain defense related items and will not be used to support or assist foreign military or space programs
- The device, technology, or software will not be directly or indirectly used for nuclear activity

Additional restrictions may apply and these exceptions cannot be used in all circumstances. There may be recordkeeping and notification requirements. University personnel should contact the Export Control Manager regarding license exceptions.

---

[22] 15 CFR §740.14
[23] 15 CFR §740.9

APPENDIX III
Department of Treasury
Office of Foreign Assets Control (OFAC)
And Other Regulations

The Office of Foreign Asset Control (OFAC) administers economic and trade sanctions based on U.S. national security and policy interests and United Nations and international mandates[24]. These programs may be country-based or list-based (weapons of mass destruction proliferation, global terrorism, narcotic trafficking). Transactions are generally prohibited between a U.S. person or entity and a person or entity in a sanctioned country (e.g. Iran, Syria, Sudan, North Korea) without a license from OFAC.

There are also prohibitions against transactions with specific entities or individuals (Specially Designated Nationals (SDN)). An OFAC license is generally required for transactions between a U.S. person or entity and a person or entity on the SDN list. Transactions can include financial transactions or the exchange of goods or services.

Both country based sanctions and the SDN list are subject to change. Specific OFAC sanctions programs determine what types of transactions are prohibited and what are allowed. Some transactions may be permitted under a general license which does not need permission from OFAC. In other cases a specific license from OFAC may be required. University personnel should contact the Export Control Manager for assistance in determining sanction and restriction applicability.

Restricted Persons

Several agencies in addition to OFAC maintain lists of individuals or entities that are barred from certain transactions with U.S. persons or entities. A U.S. Government "Consolidated Screening List" search engine is available. The Consolidated Screening list includes, but is not limited to the following lists:

- Specially Designated Nationals and Blocked Persons List (OFAC)
- Persons Named in General Orders
- AECA Debarred List (Department of State)
- Denied Persons List (BIS)
- Entity List (BIS)
- Unverified List (BIS)
- Nonproliferation Sanctions (Department of State)

Third party subscription services are also available for screening of restricted party lists ("restricted party screening" or "RPS").

Anti-Boycott Regulations

Anti-Boycott regulations are administered by the BIS (EAR) and can be found at 15 CFR 760. The "antiboycott" laws are the 1977 amendments to the Export Administration Act (EAA)[25] and the Ribicoff Amendment to the 1976 Tax Reform Act (TRA)[26]. Both of these provisions are designed to prevent any U.S. person or entity, whether in the U.S. or abroad, from participating directly or indirectly in a foreign boycott that is not sanctioned by the U.S. This prevents U.S. entities from inadvertently supporting

---

[24] 31 CFR §§ 500-599
[25] PL 96-72
[26] PL 94-455

foreign policies of other nations which may run counter to U.S. foreign policy. The regulations were implemented in response to the Arab League's boycott of Israel; however they apply to all boycotts imposed by foreign countries that are not sanctioned by the U.S.

Conduct that may be penalized under the TRA and/or prohibited under the EAR includes:

- Agreements to refuse or actual refusal to do business with or in Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality.
- Agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies.
- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person.
- Implementing letters of credit containing prohibited boycott terms or conditions.

The TRA does not "prohibit" conduct, but denies tax benefits ("penalizes") for certain types of boycott-related agreements.

<u>Exceptions</u>

There is a provision which does allow exporters to comply with the import restrictions of a boycotting country under certain circumstances. Details of exceptions can be found at 15 CFR § 760.3.

<u>Reporting Requirements and Penalties</u>

Both the EAR and TRA require reporting of requests received to support unsanctioned foreign boycotts[27]. Even if the request is refused or the language in the contract is changed, the initial request must be reported. Reporting procedures and additional information on anti-boycott regulations can be found on the BIS website: https://www.bis.doc.gov/index.php/enforcement/oac .

Other Export Regulations

Other agencies with regulations affecting export include but are not limited to:

- Nuclear Regulatory Commission, Office of International Programs
  - o Nuclear materials and equipment
  - o Regulations: 10 CFR § 110
  - o Website: http://www.nrc.gov/
- Department of Energy, Office of Export Control Policy & Cooperation
  - o Nuclear technologies and service which contribute to the production of special nuclear material
  - o Regulations: 10 CFR § 810
- Department of Justice, Drug Enforcement Administration
  - o Drugs of abuse, chemicals, precursors
  - o Regulations: 21 CFR § 1311-1313
- Website: https://www.dea.gov/Food and Drug Administration
  - o Drugs, biologics, medical devices

---

[27] 15 CFR § 760.5

- o Regulations: 21 CFR § 301 et seq. 21 CFR § 312.1106
  - o Website: http://www.fda.gov/
- Department of the Interior
  - o Endangered species
  - o Regulations: 50 CFR § 17.21-22, § 17.31-32
  - o Website: https://www.doi.gov/

Export of a controlled item without proper authorization (license or license exception) or exports violating the terms of an export license may result in criminal and/or civil penalties for the university *and/or the responsible individual (e.g. the PI)*. In some cases multiple violations of related restrictions may apply to a single export, resulting in extremely large fines. Penalties may include seizure of items, loss of export privileges, debarment from participating in future federal contracts, or jail time. It is important to note that deemed export violations are subject to the same federal penalties as physical exports. Penalties are subject to change. Details listed below were current as of 2017. For updated penalties please follow footnotes or consult the relevant agency.

Defense Articles & Technical Data
Under the ITAR and the AECA willful violations of defense controls can incur criminal penalties of up to $1,000,000 per violation and/or up to 20 years of imprisonment for the person committing the violation[28]. Civil penalties of up to $500,000 per violation may also be assessed by the Secretary of State[29].

EAR Controlled Technology
Under the EAR criminal penalties can reach $1,000,000 per violation and civil penalties can reach $250,000[30]. Imprisonment of responsible individuals can be up to 20 years.

Anti-Boycott
The Export Administration Act (EAA) provides for criminal penalties for Anti-Boycott regulations to include fines of up to $50,000 and imprisonment of up to 10 years. When the EAA is in lapse, the International Emergency Economic Powers Act (IEEPA) provides for penalties of up to the greater of $250,000 per violation or twice the value of the transaction for administrative violations, and up to $1 million and 20 years in prison for criminal violations[31].

OFAC
Criminal violations may be fined up to $1,000,000 per violation and up to 20 years imprisonment. Civil violations have a maximum penalty of $250,000 per violation[18].

Voluntary Self-disclosure
Voluntary self-disclosure of a violation can be a mitigating factor in penalty assessment, reducing penalties up to 50%. In most cases certain conditions apply, such as implementing or improving a comprehensive compliance program. Other factors which potentially affect penalty assessment include:

- If this was a first offense
- If there was a compliance program in place
- If steps were taken after discovery of the violation to correct gaps in the compliance program
- Cause of the violation; e.g. misapplication of laws, mistake of fact
- Was the violation willful or intentional
- Were steps taken to hide the violation

Information on the process of voluntary self-disclosure can be found at 15 CFR § 764.5 of the EAR and 22 CFR § 127.12.

---

[28] 22 CFR § 127, 22 USC§ 2778(c), 2780(j)
[29] 22 USC § 2778(e)
[30] PL 110-96
[31] PL 95-223; 50 USC 1701 *et seq*

APPENDIX V
Export Control Questionnaire

Name of Foreign National (FN): _____

Is this a renewal of a current H-1B Visa for employment at Alabama A&M University in the

same position and job title?   Yes   No

IF YES, ANSWER QUESTIONS IN SECTION A ONLY. IF NO, PLEASE BEGIN AT SECTION B.

A. Renewal of Current Visa

A.1. Has there been any change in role or duties of the foreign national (FN) since the last Visa approval?

Yes   No

If yes, please describe what has changed.

A.2. Are there any new or alternate funding sponsors for the work this FN will be doing since the last Visa approval? If yes, please list (e.g. NIH, NSF, Foundation…)

Yes   No

A.3. Are there any changes in foreign collaborations since the last Visa approval? If yes, please describe and list the countries involved.

Yes   No

A.4. Will the FN have access to any significant new equipment, materials, software, or technology since the last Visa approval? If yes, please describe.

Yes   No

A.5. Are there any new publication restrictions on the work the FN will be doing?

Yes   No

A.6. Are there any new citizenship requirements or restrictions on participation by foreign   nationals for the work this FN will participate in since the last Visa approval?

Yes   No

IF YOU HAVE ANSWERED SECTION A, YOU MAY SKIP SECTIONS B, C, and D and PROCEED TO THE SIGNATURE SECTION ON THE LAST PAGE.

B. General Information – **Please answer to the best of your ability based on your current knowledge of the anticipated activities of the foreign national.**

B.1 The Foreign National's work will include (**mark all that apply**):
   Basic Research
   Technician/Technical Support
   Teaching/Educational Activities
   Other (please describe)

B.2 Who is the funding sponsor for the project/employment of the foreign national (FN)? Please identify specific sponsors (e.g. NSF, USDA, DoD, industry).

B.3 Will the FN participate in activities which involve the receipt of proprietary information from a sponsor?
                          Yes   No

If yes, what type? (e.g. defense information) To your knowledge is this proprietary information export controlled?
                          Yes   No

B.4 Does the FN's work involve the design or development of encryption?
                          Yes   No

B.5 Will the FN participate in any projects known to be export controlled?
                          Yes   No

B.6 Will the FN participate in any projects involving Controlled Unclassified Information (CUI)?
                          Yes   No

If yes please give a project identifier (e.g. grant or contract number).

B.7 Will the FN be working in or near a space where there is a Technology Control Plan in place?

Yes   No

B.8 Will the FN's work involve collaborations outside the US?

Yes   No

If yes, with what countries?

B.9 Will the FN participate in projects funded by the U.S. Military (e.g. DOD) or which have direct military applications?

Yes   No

If yes please give a project identifier (e.g. grant or contract number) and attach documentation that briefly describes the aims of the project, for example the abstract or scope of work.

B.10 To your knowledge is the FN a member of or connected to a foreign military?

Yes   No

B.11 Does the FN still maintain an official connection to a foreign institution (e.g. has an official position, is enrolled as a student, or receives funding support from)

Yes   No

If yes, please name the institution and country and describe the connection.

C. Access to Possible Controlled Items

C.1. Are you aware of any equipment, materials, software, technical data, or encrypted software or hardware that would be export licensable under the **International Traffic in Arms (ITAR) Regulations** or the **Export Administration Regulations (EAR)** that the FN would   have access to (including in an open/shared lab or office environment)?

Yes   No

If yes, please indicate the type(s) of item that is (are) export controlled.

C.2. Will the FN have access to any equipment, material, software, or technical data (directly or through unrelated projects occurring in an open lab or office environment) which have been or are currently being specifically designed, developed, configured, adapted, or modified for a military, satellite, or space application?

                        Yes   No

If yes, please explain:

C.3. Please indicate the types of significant equipment the FN will be utilizing or developing in connection with his/her/their position. (e.g., examples include high speed, underwater or infra-red cameras, high-technology electronic sensors, unmanned aerial vehicles (UAVs) spectrographic instruments, chromatography instruments).

C.4. For any of the items described in question C.3., will the FN have access to technical information which would enable them to do **_all six_** of the following tasks: installation; operation; maintenance; repair; refurbishing; overhaul. (**_Note: if they are only operating and maintaining the instrument, the answer is "No"_**).

                        Yes   No

If yes, for which instruments will they have access to this information?

D.   Determination of Fundamental Research Status **If you checked ONLY Teaching/Educational Activities, you may skip section D and proceed to signature.**

D.1. Please read the U.S. Government's definition of Fundamental Research: "_Fundamental Research means basic and applied research in science and engineering the results of which ordinarily are published and shared broadly within the scientific community as distinguished from proprietary research and industrial development, design, production and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons_"

Do you consider the work this FN will be doing to be "Fundamental Research?

                        Yes   No

D.2. Will the FN participate in any activities or projects that contain restrictions (formal or informal) on publication or presentation of results in any way beyond a brief review by an industry sponsor for elimination of proprietary information?

Yes   No

If yes, please give a project identifier (e.g. grant or contract number).

D.3. Will the FN participate in any projects or activities that require approval or security clearance for foreign nationals, or that stipulate limitations on participation based on citizenship?

Yes   No

If yes, please give a project identifier (e.g. grant or contract number).

D.4. Will the FN participate in activities that involve non-disclosure agreements or confidentiality agreements with an external sponsor (i.e. the U.S government or an industry sponsor), collaborator, or third party?

Yes   No

If yes, please give the nature of the confidential subject matter.

Certification by Principal Investigator (PI) or Supervisor

I certify that the answers provided are based on knowledge of the foreign national's anticipated activities while at Alabama A&M University. The responses on this questionnaire are accurate and   complete to the best of my knowledge.

_____

Signature   *Date*

_____

Name (Please Print)   *Title*

THANK YOU FOR COMPLETING THIS QUESTIONNAIRE
PLEASE RETURN TO THE OFFICE RESPONSIBLE FOR INTERNATIONAL STUDENTS
AND SCHOLARS

APPENDIX VI

ITAR Language in Alabama A&M University Purchase Terms and Conditions

Before fulfilling this order, vendor must notify the University to obtain authorization from University's Export Control Manager if any products, technical information, service, software, or source code (collectively referred to herein as "Articles") to be provided by vendor are controlled by the Department of State, Directorate of Defense Trade Controls, International Traffic in Arms Regulations (ITAR). This vendor notification shall include the name of the Alabama A&M University point of contact for the transaction, identify each ITAR controlled commodity, provide the associated U.S. Munitions List (USML) category number(s), and indicate whether or not the determination was reached as a result of a commodity jurisdiction or self-classification process. The vendor agrees that the University shall have the unilateral and unfettered right to terminate this Purchase Order, without penalty, based on such notification. The vendor agrees that if it fails to notify the University's Export Control Manager that it is providing ITAR-controlled Articles, it shall reimburse the University for any fines, legal costs or other fees imposed by the above-named regulatory agency for any violation of export controls regarding the provided Articles.

Technology Control Plan and Briefing

ALABAMA A&M UNIVERSITY TECHNOLOGY CONTROL PLAN

The purpose of this Technology Control Plan (TCP) is to prevent unauthorized access by foreign nationals to technology controlled for export under the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). This TCP sets forth the security measures the department, principle investigator, and project personnel agree to implement in the performance of this project to prevent unauthorized foreign persons from gaining access to controlled technologies.

COMMITMENT:

It is the policy of Alabama A&M University to comply fully with all United States laws and regulations, including the laws and regulations governing the export of controlled technologies. These laws and regulations include without limitation the Export Administration Regulations ("EAR"), the International Traffic in Arms Regulations ("ITAR"), and regulations and orders administered by the Treasury Department's Office of Foreign Assets Control ("OFAC") (collectively, the "Export Control Laws").

1. Primary Responsible Party (Principal Investigator):
  Name: College/Department:
  Primary Phone:
  Primary Email:

 Administrative Contact:
  Name:
  Department:
  Primary Phone:
  Primary Email:

2. Identifying information for project
Grant/Contract number, parties, brief description

3. Description of the Item, Technology or Technical Data:

The nature of the controlled item, technology or technical data. Include export classification (USML or ECCN number) and if possible who classified it.

4. Physical Security Plan

Location
Project data and/or materials must be physically protected from access and observation by unauthorized individuals.

[Describe the physical location of each sensitive technology/item, to include building and room numbers.]

Physical Security

[Provide a detailed description of the physical safeguards that will be put in place to prevent unauthorized persons from accessing the technology/information. Physical safeguards may include locked doors, locked cabinets/drawers, key card or badge access, escorts and similar physical restrictions.]

In addition to the foregoing, the following measures will be observed to prevent inadvertent access by unauthorized foreign nationals to the export-controlled technology/information:

- Hard copy documents containing export-controlled information will be clearly labelled as "Export Controlled" and secured from unauthorized access, for example stored in a locked drawer when not in use.

- Technical data will not be printed unless necessary, and if printed will be promptly retrieved, and will not be left in the open where unauthorized persons can access it.

- Documents containing export-controlled information will be shredded prior to disposal.

- Unauthorized individuals will be prevented from visually accessing export controlled information, for example by viewing it on a computer monitor when it is in use.

5. Information Security

Controlled electronic information must be secured by appropriate measures, such as User IDs, password control, SSL etc. An example would be database access managed via Virtual Private Network (VPN) for authorized persons using 128-bit Secure Sockets Layer (SSL) or other advanced federally approved encryption technology.

[Describe the structure of your IT security set up at each item/technology location and how you will prevent access by unauthorized persons.]

Information security procedures may include the following:

- Export-controlled technical data shared within the research team must be distributed via secure media. Cloud services such as Gmail are not secure and therefore should not be used to communicate controlled information.

- Export-controlled technical data will not be stored on computers unless the computers are locked and password-protected when unattended. An exception may occur only if the files themselves are protected, for example with passwords or other acceptable means.

- Discussions about the project or work product are limited to authorized personnel and are held only in areas where unauthorized personnel are not present.

- Removable memory storage devices may be used for data back-up only within the designated secure area. When not in use, back-up drives must be clearly marked ("Export Controlled") and stored in a designated secured location (e.g. locked drawer or cabinet).

- All electronic storage media must be secured or destroyed upon completion of the project.

6. Personnel Screening

[Identify all personnel who will have access to export-controlled technology/information related to this project.]

Person   **Citizenship**

This TCP will be amended if personnel changes occur. All personnel assigned to this project and all visitors afforded access to controlled information or technology must be screened against the U.S. Government's denied parties lists prior to being afforded such access. Documentation of screening results will be provided by the Export Control Manager.

7. Training and Awareness

All personnel with access to export-controlled technology or information will be briefed on this Technology Control Plan and must certify their understanding of the TCP by signing the attached "Briefing and Certification on the Handling of Export-Controlled Information." Additional export control training may be required by the Export Control Manager on a case-by-case basis.

8. Ongoing Compliance Assessments

The Export Control Manager may conduct periodic reviews and/or training to assess or improve compliance with the TCP. Any changes to procedures or personnel identified in this TCP must be approved in advance by the Export Control Manager. Contact the Export Control Manager with questions or concerns at research.compliance@aamu.edu.

9. Project Termination

The obligations of this TCP continue as long as the technology/information remains in the University's possession. Disposition of export-controlled items, equipment or information should be coordinated with the Export Control Manager. All records pertaining to the export-controlled technologies/information will be retained in accordance with University policy and all applicable federal regulations.

10.   TCP Periodical Review

All TCPs must be reviewed by the PI on a periodic basis, approximately annually. This review includes ensuring that all sections of the TCP are up-to-date. Any changes to personnel or control measures must be reported to the Export Control Manager so the TCP can be revised accordingly.

CERTIFICATION:
I hereby certify that I have read and understand the terms of this Technology Control Plan. I agree to follow the procedures set forth herein and to take other actions as necessary to prevent unauthorized access by foreign persons to the controlled technologies. I understand that I may be held personally liable for civil and criminal penalties, up to and including incarceration, if I disclose any export-controlled information to unauthorized foreign persons.

PRINTED NAME	SIGNATURE	DATE

Approved: Date:
    [Must be approved by the Export Control Manager]

<u>BRIEFING AND CERTIFICATION ON THE HANDLING AND PROTECTION OF EXPORT CONTROLLELD INFORMATION</u>

Briefing
This research project involves the receipt and/or use of information controlled for export under the International Traffic in Arms Regulations (ITAR) or the Export Administration regulations (EAR).

Controlled Information
In general, "Controlled Information" means any information relating to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing, or use of items with a capacity   for military application. Technology or information may be export-controlled even if the   intended end use is civilian in nature. The term does not include basic marketing information,   general system descriptions, information already in the public domain, or information   concerning general scientific, mathematical, or engineering principles commonly taught in   schools, colleges and universities.

International Traffic in Arms Regulations (ITAR)
The International Traffic in Arms Regulations (ITAR) control the export-and re-export of equipment, software and technical data designed primarily for military, space or satellite applications. The ITAR also control the provision of certain defense-related services. Under the   ITAR, it is unlawful to transfer controlled information outside the U.S. or (whether in oral, visual   or hard copy form) to any foreign person inside the U.S. ("deemed" exports). A foreign person is   someone who is not a U.S. citizen or permanent resident alien (green card holder) of the United   States. The law recognizes no exceptions for students.

Export Administration Regulations (EAR)
The Export Administration Regulations (EAR) control the export and re-export of equipment, software and technical data having both civilian and military applications ("dual use" technologies). Unlike the ITAR, the EAR's prohibitions can vary depending upon a foreign person's home country. Under the EAR, transfer of controlled information to certain countries or   foreign nationals from those countries who are within the U.S. may require a license.

Penalties
Researchers may be held personally liable for violations of the ITAR and EAR. Both the ITAR and EAR authorize criminal and civil sanctions. Criminal sanctions under the ITAR include fines of up to $1,000,000 and 10 years' incarceration per violation. Criminal sanctions under the EAR   include fines of up to $1,000,000 and incarceration up to 20 years per violation.

Reasonable Care
You must exercise care in using, sharing and safeguarding export-controlled materials or technical data with others. Unless authorized by the appropriate government agency and notified to that effect by Alabama A&M University's Export Control Manager, you may not export   controlled materials or technical data to which you have been granted access. If you foresee the need to export such information to a foreign country or foreign person (including,

but not limited to, any University employees or students) as a part of your research at Alabama A&M University, please inform the Export Control Manager (research.compliance@aamu.edu) immediately to determine if an exemption is applicable or if a license or written assurance is needed.

<u>CERTIFICATION</u>

I understand that my participation on the research project(s) listed may involve the receipt or use of export-controlled technology, items, software or technical data, and that it is unlawful to transfer, send or take export-controlled materials or technology out of the United States. I understand that I may not disclose, orally or visually, or transfer by any means, export-controlled technology or technical data to a non-U.S. person located inside or outside the U.S. without a license or applicable exemption as determined by WU's Export Control Manager. I understand the law makes no specific exceptions for non-US students, visitors, staff, postdocs or any other person not pre-authorized under a TCP to access export controlled materials or data.

I have read and understand the conditions of this certification. I am electing to participate in the research cited, and I agree to follow the procedures outlined in the Technology Control plan. I understand I could be held personally liable if I unlawfully disclose export controlled technology, technical data, materials or software to unauthorized persons. I will address any questions I have regarding the designation, protection or use of export-controlled information with the Export Control Manager at research.compliance@aamu.edu.

Person	Signature	Date

Approved by:_____ Date:_____

Original signed forms for all project personnel (including PI) must be retained in the Department along with the TCP (also signed by all project personnel.) Also send a copy of all signed forms to the Export Control Manager at research.compliance@aamu.edu.