Export Compliance Program Manual

Export control laws are complex, dynamic, and fact specific. Regulations, rules, and lists for specifying who or what is considered export sensitive and where export controls apply are subject to change. This Manual is intended to provide an overview of basic export control information. It should not be relied upon exclusively, nor should it be construed as legal advice. Any questions should be directed to Export Control export@arizona.edu.

THE UNIVERSITY OF ARIZONA

Table of Contents

I. MANAGEMENT COMMITMENT

The University is committed to complying with U.S. export controls laws and regulations including the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and the Office of Foreign Assets Control (OFAC) regulations. All individuals working at the University of Arizona who work with, or have access to, export-controlled technical data, software, materials, and equipment are required to be familiar with and adhere to the U.S. export control laws and regulations.

II. ROLES and RESPONBILITIES

The following is a summary of roles and responsibilities outlined in the policy:

All Employees and students: Supporting research, developing relationships, and participating in the worldwide academic and business community to further the pursuit of knowledge is a critical component of the University of Arizona mission. All employees, students, and other individuals working at University conduct their affairs in accordance with applicable U.S. laws and regulations, **University Policy** and consistent with the highest standards for research integrity and ethics.

Export Control: Responsible to develop and implement university-wide policies and procedures, advise, train, and oversee institutional compliance with export control regulations. The Director is designated as the University's primary Empowered Official with the authority to make export controls determinations and government license submissions on behalf of the institution. Export Control will respond to reports of potential violations of export control regulations, inform federal agencies, and lead efforts to respond to violations. Export Control will also provide guidance on next steps with identified restricted parties.

Primary Investigators (PIs) on export-controlled projects are responsible for:

- Identifying activities that may intersect with export control regulations;
- Maintaining a current export control training certification;
- Confirming all project personnel have completed training and are cleared to access export-controlled items; and
- Notifying Export Control of potential violations.

Central administrative units, departments, and colleges: Coordinate with Export Control on centralized procedures for **Restricted Party Screenings** and identifying international collaborations, travel, services, and online study abroad requiring OFAC or other licenses. For example, all individuals affiliated with the University who work with international persons and entities must confirm via Restricted Party Screening and consultation with Export Control that activities are permitted with collaborators.

Liaison Program: Export Control works closely with various Liaison Administrators across campus. Liaisons assist Export Control in identifying/resolving export control issues. Export Control established checklists, forms, and procedures to identify export control concerns. Examples of "red flags" include publication restrictions, foreign person restrictions, and projects related to military and space. Reference the checklist and forms in **Appendix C.**

III. EXPORT CONTROL OVERVIEW

Export controls are federal laws that govern the transmission of controlled items and associated technical data to foreign nationals. There are also federal regulations regarding providing services, traveling to, or working with individuals or entities from sanctioned or embargoed countries. These federal regulations not only affect items that are utilized by UA personnel, but can also affect whom the UA engages with on campus as well as around the world.

Export control laws and regulations affect various University activities including, but not limited to, conducting research (sponsored and unsponsored), international travel, publishing research, procurement, hiring non-U.S. persons, sponsoring foreign persons (e.g., visiting scholars), collaborations with non-U.S. individuals or entities, international shipments, non-disclosure agreements, and certain services to embargoed or sanctioned countries.

The **Export Administration Regulations** (EAR) and the **International Traffic in Arms Regulations** (ITAR) govern not only the shipment or transfer of export-controlled items (e.g., technical data, software, materials, and equipment) outside the U.S., but also access to certain export-controlled items to non-U.S. persons **within** the U.S. In addition, the **Office of Foreign Assets Control** (OFAC) regulations impose sanctions and embargoes on transactions or exchanges with designated countries, entities and individuals.

The export regulations are in place to protect not only the economic vitality of U.S., but to prevent the diversion of technologies used against U.S. interests. The University of Arizona recognizes these laws support vital national security, economic, and foreign policy interests.

International Traffic in Arms Regulations (ITAR)

The Department of State's responsibility for the control of the permanent and temporary export and temporary import of defense articles and services is governed by **22 U.S.C. 2778** of the Arms Export Control Act (AECA) (Reference: **U.S. Munitions List - General Categories**).

Export Administration Regulations (EAR)

The **Department of Commerce's Bureau of Industry and Security** (BIS) is charged with the development, implementation and interpretation of U.S. export control policy for dual-use commodities, software, and technology (Reference: **Export Administrative Regulations and Commerce Control List**).

Office of Foreign Assets Control (OFAC)

The **Office of Foreign Assets Control** ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in the proliferation of weapons of mass destruction, and other threats to national security that impact the foreign policy or economy of the United States (Reference: **OFAC Country Sanctions Programs List**).

IV. REGISTRATION TO SUBMIT LICENSES

Generally, any U.S. person or entity that manufactures, brokers, or exports defense articles or services must be registered with the Directorate of Defense Trade Controls (DDTC). Registration is required prior to applying for a license or taking advantage of some license exemptions. Once the registration is complete, an exporter may apply for an export authorization by submitting a relatively simple license application for the export of defense articles or technical data; or a complex license application, usually in the form of a Technical Assistance Agreement ("TAA"), for complex transaction that will require the U.S. entity to provide defense services.

The University of Arizona is registered with the DDTC and Export Control is responsible for license applications on behalf of the University. A license or government authorization may be required prior to exporting (including deemed exports) to a foreign individual or entity. For example, a license or exemption is typically required for a foreign national to work on ITAR-controlled research.

V. INTERNATIONAL ACTIVITIES

Federal Export Laws and Regulations

Federal regulations and sanctions promulgated and enforced by various federal agencies [1] prohibit the unlicensed export of specific technologies and items and payments to certain entities and individuals for reasons of national security or protection of trade. Most research conducted on U.S. university campuses is considered Fundamental Research and is excluded from these regulations. However, some university activities or research may require ***prior*** government authorization (e.g., working with certain export-controlled technologies, transactions, and exchanges with designated countries, and collaborating with non-U.S. citizens or entities). The consequences of violating these regulations can be severe - ranging from loss of research contracts to monetary and criminal penalties for the individual and/or organization.

Travel Outside the United States

Travel outside the United States can trigger the need for a federally issued license(s), depending on the proposed destination, what you plan on taking with you, the nature of the project associated with the travel, and with whom you will be working. The following should be considered prior to travel:

- Laptops, software, and other equipment should be vetted prior to travel for possible export licensing issues (this includes but is not limited to hardware, equipment, technology, technical data, schematics, blueprints or other project-related information, and encryption capabilities).
- Presentations to be given at a conference or meeting should be vetted for possible export control data, including any accompanying materials or handouts.
- In some cases it is possible to use a license exemption/exception in lieu of a license.
- If a license or license exception is required, it must be in place ***prior to*** travel. If an exception is not applicable and a license is required, a license can take up to eight weeks to process once submitted. Thus, **planning and coordination are essential**.

[1] Department of Commerce, Bureau of Industry and Security (BIS) administers the Export Administration Regulations (EAR) commonly associated with the regulation of dual-use commodities contained on the Commerce Control List (CCL).

Department of State, Directorate of Defense Trade Controls (DDTC) enforces the International Traffic in Arms Regulations (ITAR) regulating the export of military and space technologies contained on the United States Munitions List (USML).

Department of Treasury, Office of Foreign Asset Control (OFAC) oversees U.S. embargoes and economic sanctions on various foreign countries.

- If the data or item is ITAR controlled**,** there is a policy of denial to export or take items to certain countries (e.g., China, Cuba, Iran, Iraq, Russia, Somalia, Syria, and Venezuela).
- The University of Arizona will **NOT** apply for an export license if the data, equipment, software, or information is ITAR controlled and is intended for export to a proscribed country or person.
- Agencies, entities, and individuals you will be collaborating with should be screened through Visual Compliance prior to travel to determine if they are on a "denied" list. A federal license would be required and could, in fact, be denied.
- All licenses and license exceptions will be processed by the Export Control team in collaboration with the PI/employee requiring the license.

OFAC Regulations

The purpose of the OFAC regulations is to enforce embargoes and economic sanctions. In general, the OFAC regulations prohibit exports to certain sanctioned/embargoed countries such as Iran, Cuba, Sudan, North Korea, and Syria. **OFAC considers providing anything of value or a service to Iran or the government of Iran would require prior government approval.** For example, giving a professional presentation, whether it contains materials controlled under ITAR or EAR, is deemed under OFAC to be a "service" and "something of value" provided to the recipient audience. In addition, there are other considerations which vary by country:

- There are OFAC restrictions related to taking online courses abroad in certain sanctioned counties. Licenses to provide a service to sanctioned countries are required under some circumstances. There may also be licensing requirements for software and other items. **OFAC Licenses - Online Courses in Sanctioned Countries**
- Most activities in Iran will require an OFAC license which can take months to process. Activities in embargoed and sanctioned countries may require a license from Commerce, OFAC, or both. **There is a presumption of denial for anything ITAR-controlled.**

- For example, attending a conference in Iran (OFAC considers this to be an "import") or speaking at a conference in Iran (providing a service or something of value) requires a license. An OFAC license for Iran generally takes six to nine months (or longer) to process once submitted.

- Any technical discussions, *formal or informal*, *could* require a license and would be prohibited ***prior to*** the receipt of the necessary license(s).

- If an employee travels to any sanctioned country on their own time, **the individual may not take or send anything university-owned** such as equipment, software, technology, or data, or represent the university in any capacity.

Duo Restricted in Embargoed Countries

The UA agreement with **Duo** does not allow UA users to access or use Duo's services in a U.S. embargoed country without U.S. government authorization. In addition, there are export control regulations that impact the use of Duo in embargoed countries. Cuba, Syria, and Iran are the comprehensively embargoed countries. There is an OFAC **General License D-1 Iran** that covers the use of Duo in Iran. No additional paperwork is required.

To access or use Duo's services in Cuba requires signed documentation prior to travel. The Consumer Communications Devices ("**CCD**") license exception form should be signed by the traveler and sent to Export Control for signature (**export@arizona.edu**). The form will be returned and should be kept with the traveler during the trip. Documentation must be kept for five years.

Travel Authorization Process

All University of Arizona personnel traveling internationally on University business are required to complete and submit a Travel Authorization form, register each trip in the **University International Travel Registry**, and receive approval prior to travel.

License Exception Forms

License exception forms may be needed when taking items or equipment abroad.

TMP License Exception Form If a Commerce license is required, this form should be used in lieu of a license (applicable for most countries) if the traveler is taking University owned equipment, such as a laptop. This exception is not applicable for anything ITAR controlled; a license from State would be required.

BAG License Exception Form If a Commerce license is required, this form should be used in lieu of a license (applicable for most countries) if the traveler is taking a personal laptop or other equipment that contains University of Arizona project data. This exception is not applicable for anything ITAR controlled; a license from State would be required.

CCD License Exception Form License exception CCD authorizes the export or reexport of commodities and software controlled under the Export Administration Regulations (EAR) to Cuba or Sudan under specific conditions. Only certain commodities and software are authorized.

For additional information see **FAQs - International Travel**

Accessing Data While Abroad: Accessing export-controlled data abroad is considered an export, including opening an encrypted email with ITAR or export controlled data or accessing the data even on the University server through the VPN. University personnel must coordinate in advance with Export Control if they need to access export-controlled data abroad. A license or license exemption is required in most cases. However, there are some countries where a license or license exemption would not be granted.

VI. RESTRICTED PARTY SCREENINGS

To remain compliant with federal regulations, the University of Arizona conducts Restricted Party Screenings (RPS) to help prevent illegal transactions with restricted parties.

Visual Compliance is an online tool used to screen the various lists of restricted individuals and entities. University representatives in colleges and administrative units have direct access to the Visual Compliance system. Contact export@arizona.edu to determine your unit's liaison(s), to request direct access, or for assistance with occasional screenings. New users receive access after submitting a completed **Code of Conduct form**.

Reference: **Chart of University Screening Responsibilities**

The system is user friendly and training is not required but available upon request. We recommend consulting the following resources:

- **RPS Basics with Visual Compliance**
- **Using the "Resolve Match" feature**
- **Screening Tip Sheet**

VII. RED FLAGs - EXPORT CONTROL REVIEWS

Export Control in coordination with the colleges and the Sponsored Projects and Contracting Services, reviews agreements for potential export control issues (red flags). The University **Export Control review checklist** is required **prior to acceptance** of agreements with any of the following red flags:

- Publication, access, and dissemination restrictions in the agreement;
- Foreign party restrictions stated in the agreement;
- International travel to countries subject to U.S. embargoes and sanctions;
- Sponsor is providing export-controlled technology, technical data, or equipment;
- Non-U.S. students or visiting scholars participating in a restricted project;
- Project is sponsored by the federal government or defense contractor;
- Project is military, space-related, or has other implications to national security;
- Project will be conducted abroad or with a foreign sponsor or collaborator;
- Sponsor /research/collaborator is in Cuba, Iran, North Korea, Sudan, or Syria; and
- Any shipment of goods, services, information, or technology abroad.

VIII. EXPORT CONTROL CLASSIFICATION PROCESS

Export Control reviews the checklist (red flags), the agreement, and other documentation to make an export control determination. Export Control frequently obtains clarification from the PI and/or the Sponsor on the project parameters and any data or equipment that will be exchanged or generated. Export Control researches the regulations starting with the ITAR and then the EAR to make a classification determination. If export controls are applicable, the project could require a Technology Control Plan (TCP) and/or an export license prior to commencement of activity.

While Directorate of Defense Trade Controls (DDTC) has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify the item. If doubt exists as to whether an article or service is covered by the U.S. Munitions List, upon written request in the form of a Commodity Jurisdiction ("CJ") request, DDTC will provide advice as to whether a particular article is a defense article subject to the ITAR, or a dual-use item subject to Commerce Department licensing. Determinations are based on the origin of the technology (i.e., as a civil or military article), and whether it is predominantly used in civil or military applications. University employees should contact the University of Arizona's Export Control team for assistance with classification of an item. If the University of Arizona needs to obtain a CJ determination, the Export Control will file the CJ request with DDTC.

IX. TECHNOLOGY CONTROL PLANS

Technology Control Plan: The purpose of a TCP is to control the visual, physical, or electronic access by unauthorized non-U.S. Persons to certain export-controlled data, items, materials, equipment, and software. Before export-controlled work can begin or export-controlled data can be received, each project member must complete online export control training and participate in a TCP briefing from Export Control.

If Export Control determines that a project is export-controlled, Export Control will work with the PI to develop and implement a TCP to secure the controlled technology/items from access from unlicensed non-U.S. citizens. The TCP will include:

- A commitment to export control compliance;
- Identification of the export control categories and controlled technologies/items;
- Identification and nationality of each individual participating in the project;
- Appropriate physical and informational security measures;
- Procurement and international shipment requirements;
- Personnel screening measures;
- Appropriate security measures for and following project termination;
- Export control training requirements; and
- Compliance assessment – audits.

The TCP will include physical and informational security measures appropriate to the export control categories involved in the project. Examples of security measures include:

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

- Time Blocking: Project operation may be restricted to secure time blocks when unauthorized individuals cannot observe or access.

- Visitor: Use of visitor logs to track access to the restricted area.

- Marking: Export-controlled information must be clearly identified and marked as export-controlled.

- Personnel Identification: Individuals participating in the project *may* be required to wear a badge, special card, or other similar device indicating their access to designated project areas.

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

- Electronic Security: Project computers, networks, and electronic transmissions should be secured and monitored through User Ids, password controls, 256-bit Secure Sockets Layer encryption or other federally approved encryption technology. Database access should be managed via a Virtual Private Network.

X. TRAINING

University of Arizona employees working on an export-controlled project with a TCP must complete the initial export control training **prior to working on** a project or accessing export-controlled information. Agreements will not be processed by Contracting Services until training is confirmed as current and the TCP is in place.

- Refresher training is required every two years as long as an individual is on the TCP.
- PIs conducting research secured with a TCP are responsible for ensuring all personnel complete the required training.

Initial Training- Export Control in a University Setting

Use **this link to log in and select enroll** in the course with your university credentials. Completing this course will automatically enroll you in the Export Control Certification. For assistance with system questions please contact **Research-Training@email.arizona.edu**.

Refresher & Additional Training

A refresher training is required every two years to maintain the Export Control Certification and remain on a TCP. This requirement can be completed by attending a live presentation or online options. ***The learning platform will email you next steps to meet this requirement.***

- Export Control: A Quick Refresher provides an overview for the researcher with export control experience needing to renew the Export Control Certification.

- **Export Compliance Part 1** and **Export Compliance Part II** expand the introduction of export regulations and are recommended after the initial training, Export Control in a University Setting. To access, click the link, log in, then click "enroll" on the course.

The Bureau of Security (BIS) offers **Export Administration Regulations (EAR) trainings** that do **not** fulfill University training requirements.

XI. AUDITS

As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process to review procedures. The TCP contains a self-audit checklist to be completed by the Project Director/PI and (or) his/her designee and any concerns should be shared with Export Control. The importance of self-reporting potential issues is emphasized during training sessions and during the TCP onboarding.

Export Control annually conducts a formal TCP audit and may periodically evaluate and recommend or require training to maintain compliance with TCP procedures. The purpose of the reviews is to identify possible violations and deficiencies in training, procedures, personnel, handling of data, etc. The goal of the audit is to identify and correct any issues and self-report any violations should that be necessary.

XII. RECORD KEEPING

The University of Arizona is required to maintain records related to exports for five years after the license or other approval has expired. Export Control maintains records related to all exceptions/exemptions, applications, and licenses for five years after the licenses or other approvals have expired.

XIII. PURCHASING and SHIPPING

The following provides guidance on processing University of Arizona purchases in accordance with U.S. Export Regulations. Contact Export Control with any questions. Click on hyperlinks below for details:

P-Card Purchases: Purchases of equipment, tooling, or services in an amount less than $10,000 are generally made using University P-Cards. P-card purchases can be made by department personnel (purchaser). P-card purchases do not require prior review by Procurement and Contracting Services (PACS).

Requisition Purchases: Purchases of equipment, tooling, or services in an amount greater than $10,000 require the department personnel (purchaser) to submit a requisition form to the PACS office. In addition to the requisition form, purchasers are required to provide three supplier sources. If only one source is available, a Sole Source Verification Form must be submitted.

Shipping & Receiving: Export Control should be notified before the export of any items outside the U.S or to a foreign person within the United States. Items may not be shipped abroad until a determination has been made as to whether an export license is required.

XIV. PROCESS FOR REPORTING VIOLATIONS

It is the responsibility of Export Control to determine if a University activity has export control issues and put procedures in place to protect the University activity from unauthorized access by non-U.S. persons. If unauthorized access to certain export-controlled data, information, materials, software, or equipment has been given to non-U.S. persons; or services, equipment, data, or other items have been provided to a "denied entity" then Export Control must investigate and report to appropriate government agency if deemed to be a suspected violation.

Procedures

1. If the Export Control receives notification that a suspected violation has occurred, or the Export Control discovers a suspected violation during a TCP audit, the activity must cease immediately.
2. Export Control will immediately notify the Office of General Counsel (OCG) and the Vice President, Operations, Research, Innovation and Impact if a suspected violation has occurred.
3. In conjunction with the OGC, Export Control will investigate the purported violation per the requirements of the applicable government agency. See references below.
4. Individuals involved with the alleged violation will be interviewed and documentation regarding the suspected export violation collected per the requirements of the applicable government agency.
5. In conjunction with the OGC, if Export Control determines a suspected export violation occurred, the suspected violation will be reported to the appropriate government agency by either Export Control or the OGC.
6. The activity can be reinstated only after being deemed as not an export violation by the University investigation, or the appropriate government agency has determined the activity to not be an export control violation, or a government authorization (license) has been obtained for the activity.

XV. PENALTIES FOR VIOLATIONS

Generally, any person or entity that brokers, exports, or attempts to export a controlled item without prior authorization, or in violation of the terms of a license, is subject to penalties. Violators may incur both criminal and civil penalties. Although there is a maximum amount for a civil or criminal penalty, the actual penalty imposed is often multiplied. For instance, each export might be considered a separate violation, and the federal agencies will often find multiple violations of related restrictions in connection to each export (e.g., export without a license, false representation, actions with knowledge of a violation, etc.). A series of violations occurring over a period of time may result in hundreds of thousand or even millions of dollars of penalties.

The U.S. Government can also seek to criminally prosecute conduct where violations are willful and knowing. Such violations may reach $1,000,000 and imprisonment of up to 20 years. In addition, where there is egregious conduct by the offender, the federal government may suspend the export privileges of a company.

In assessing penalties, DDTC, BIS, and OFAC will consider a number of factors, both aggravating and mitigating. Mitigating factors include (1) whether the disclosure was made voluntarily; (2) whether this was a first offense; (3) whether the company had compliance procedures; (4) whether steps were taken to improve compliance after discovery of violations; and (5) whether the incident was due to inadvertence, mistake of fact, or good faith misapplication of the laws. Aggravating factors include: (1) willful or intentional violations; (2) failure to take remedial action after discovery; (3) lack of a compliance program; and (4) deliberate efforts to hide or conceal a violation.

XVI. DISCIPLINARY PROCESS

In recognition of the seriousness of non-compliance with export controls, The University of Arizona will address non-compliance in accordance with University policy. Further, all University of Arizona employees responsible for export controls compliance or participating in export-controlled projects must be aware of the substantial criminal and civil penalties imposed for violation of the export regulations including personal liability, monetary fines, and imprisonment.

XVII. EMPLOYEE PROTECTION

No individual shall be punished solely because he or she reported what was reasonably believed to be an act of wrongdoing or export control violation. However, a University of Arizona employee will be subject to disciplinary action if the employee knowingly fabricated, knowingly distorted, or knowingly exaggerated the report.

University faculty, staff, or students should contact Export Control and/or the Ethics Hotline at 866-364-1908 or online at **https://compliance.arizona.edu/hotline**.

APPENDIX A – KEY TERMS and DEFINITIONS

Export: An export is the transfer of export-controlled data, items, equipment, materials, and software or providing a defense service to a non-U.S. Person or entity. An export can occur in a number of ways, such as; a physical shipment, hand-carrying an item out of the U.S., email transmission of data, presentations, discussions, or visually accessing export-controlled data.

Deemed export: A deemed export is the release or transmission in any form of export-controlled technology or software code within the U.S to anyone who is not a U.S. Person.

Exclusions: For University research, there are three ways that technical information may qualify for an exclusion from the deemed export rule. Information is excluded if it:

- Is published or disseminated in the Public Domain
- Arises during, or results from, fundamental research
- Is educational information released by instruction in catalog courses or associated teaching laboratories of academic institutions.

Technical data: is a term defined in the International Traffic in Arms Regulations (ITAR) as information, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles and software directly related to defense articles.

Technology: is defined by the Export Administration Regulations (EAR) as specific information necessary for the "development", "production", or "use" of a product. Technical data and technology may take the form of blueprints, drawings, manuals, models, specifications, tables, formulas, plans, instructions, or documentation.

Defense article: Defense articles are all items, data specifically designed, developed, configured, adapted, or modified for a military application. Defense articles are listed on the U.S. Munitions List (22 CFR Section 121.1).

Defense service: A defense service is furnishing of assistance to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; or the furnishing to foreign persons of any technical data controlled whether in the United States or abroad.

Dual use item: These are items and associated technologies that are commercially available and also have military or proliferation applications. Items determined to have a dual capability are enumerated in the Commerce Control List.

Commodity Jurisdiction: While Directorate of Defense Trade Controls (DDTC) has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages exporters to self-classify the item. If doubt exists as to whether an article or service is covered by the U.S. Munitions List, upon written request in the form of a Commodity Jurisdiction ("CJ") request, DDTC will provide advice as to whether a particular article is a defense article subject to the ITAR, or a dual-use item subject to Commerce Department licensing. Determinations are based on the origin of the technology (i.e., as a civil or military article), and whether it is predominantly used in civil or military applications.

Technology Control Plan: A TCP is a protocol that outlines the procedures to secure certain export-controlled items (technical data, materials, software, or hardware) from unauthorized use, access, and observation by non-U.S. persons. Export Control, with assistance from the Principal Investigator (PI), will develop a TCP that is designed for the specific project. The PI is the ultimate responsible party for adherence to the TCP by project personnel. All project personnel listed on the TCP are required to complete export control training every two years. The TCP remains in effect for as long as UA retains the export- controlled data or item, even if the project is over. Export Control will conduct an annual audit to ensure compliance with the TCP.

U.S. Person: An individual with U.S. citizenship, Permanent resident alien (Green Card holder) or protected individual status such as refugees and asylees. Corporations or organizations incorporated in the United States are U.S. Persons for purposes of the ITAR and EAR. It is also any business entity incorporated to do business in the United States.

Foreign entity: A foreign entity is any corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments. A person (even a U.S. citizen) is considered a foreign person if they work for or represent a foreign entity.

Bona fide full-time employee: Export control regulations exempt disclosures of unclassified technical data in the United States by U.S. universities to foreign nationals where:

- **the foreign national is the University's bona fide full-time regular employee;**
- the employee's permanent abode throughout the period of employment is in the United States;
- the employee is not a national of an embargoed country; and
- the University informs the employee in writing that information disclosed may not be disclosed to other foreign nationals without governmental approval.

EXPORT CONTROL EXCLUSIONS and IMPLICATIONS

Exclusions: Research is generally not subject to export control if it qualifies for one of three exclusions:

(1) Fundamental research exclusion;
(2) Education Information Exclusion; and
(3) Public domain exclusion.

Fundamental Research Exclusion

The fundamental research exclusion is a broad-based general legal exclusion to protect technical information (but not tangible items) involved in research from being controlled by export controls. Research qualifying as "fundamental research" is not subject to export controls.

- The EAR definition of fundamental research means 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.
- The ITAR defines fundamental research as basic and applied research in science and engineering conducted at accredited U.S. institutions of higher education where the resulting information is ordinarily published and shared broadly within the scientific community. Such research can be distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary reasons or specific national security reasons.
- University research will not qualify as fundamental research if the university or researcher accepts any restrictions on the publication of the information resulting from the research, other than limited prepublication reviews by research sponsors to prevent inadvertent divulging of proprietary information provided to the researcher by sponsor or to ensure that publication will not compromise patent rights of the sponsor.

NOTE: If the U.S. Government funds research and specific controls are agreed on to protect information resulting from the research, then information resulting from the project will not be considered fundamental research. Such controls are usually contained in contractual clauses. (e.g., publication "approval" by the Government; restrictions on dissemination of information to non-U.S. citizens or other categories of persons; or restrictions on participation of non-U.S. citizens or other categories of persons in the research).

Educational Information Exclusion

The educational information exclusion covers commonly taught in courses listed in catalogues and associated teaching laboratories of academic institutions in the United States.

Public Domain Exclusion

The public domain exclusion applies to information that is published and that is generally accessible or available to the public through:

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

APPENDIX B – CONFIDENTIAL UNCLASSIFIED INFORMATION (CUI)

CUI OVERVIEW

Controlled Unclassified Information (CUI): Executive Order 13556 "Controlled Unclassified Information," (the Order), issued on November 4, 2010, established the CUI program, which standardizes and simplifies the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. The National Archives and Records Administration (NARA) serves as the Executive Agent to implement this order and oversee agency actions to ensure compliance.

National Institute of Standards and Technology (NIST): **NIST 800-171 Rev. 2**: The National Institute of Standards and Technology **Special Publication 800-171** provides agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) when resident in Non-Federal Information Systems and Organizations. ***There are over one hundred security requirements in the NIST; this document is summary in nature and not an exhaustive list. See the NIST for complete details***.

DFAS 252.201-7012: Safeguarding Covered Defense Information and Cyber Incident clause: This clause requires the university to implement security measures as outlined in the **NIST 800-171**. In the event of a cybersecurity incident, the university's responsibility under **DFARS 252.204-7012** is to report the incident to the DoD within 72 hours. The university should preserve and protect images of all known affected information systems identified in this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report.

DFARS 252.204-7000 clause: Disclosure of Information restricts the release of information unless the information is already in the public domain, the Prime Contracting Officer has given prior written approval, or the results during the performance of the project involved no covered defense information and determined by the Contracting Officer to be fundamental research.

IDENTIFYING CUI

The University of Arizona's Export Control team works closely with the Contracting Office to identify contracts with NIST requirements or clauses with publication restrictions **(e.g., DFARS 252.204-7012 and 252.204-7000)**. Export Control is also alerted when there are similar safeguards/restriction clauses in contracts that are not sponsored by Department of Defense (NASA contracts often have similar clauses).

An **export control checklist** is used in the evaluation process. The three-part checklist must be completed by the PI, Contracting Office, and Export Control. The checklist highlights DFARs clauses in addition to potential export control red flags.

If both the 7000 and 7012 clauses are in an agreement, the University/Sponsor can go back to the prime contracting officer and ask if the University of Arizona's portion of the work is fundamental in nature. If the University receives written confirmation from the prime contracting officer that the university's work in fundamental research, the CUI clauses are nullified.

Once a project is determined to be CUI, it is managed under a security plan. Export Control worked closely with the IT-CUI team to develop "The Plan," a joint Technology Control Plan and System Security Plan. This plan outlines the security measures researchers and staff must follow in order to protect the CUI data.

University Information Technology Support (UITS)-CUI at the University of Arizona deploys Amazon GovCloud (AWS), which can be accessed by the following devices.

Access Type	Laptop/Desktop	Upload/Download Data	Store Data Locally
"Red Machine"	Currently UA-owned/used	**NO** *Data **only** in AWS /CUI environment*	**NO**
A "red machine" is a UA-owned/issued computer which allows the individual to log into and work in the CUI environment. No information can be uploaded to or downloaded from the CUI environment. No CUI data can be stored locally on this computer.			
"Green Machine"	UA-UITS hardened & provided	**YES**	**YES**
A "green machine" is a UA-owned laptop provided by UITS which allows the individual to not only work within the environment, but also information can be pushed to or pulled from the environment. The "green machine" is hardened to meet the NIST 800-171r2 standards. CUI information can be stored and processed locally on the "green machine."			

See below links for more information or contact the CUI team at: **cui-support@list.arizona.edu**

- **https://it.arizona.edu/cui**
- **https://rgw.arizona.edu/sites/default/files/cui_faq_01.11.2021.pdf**

APPENDIX C – FORMS and CHECKLISTs

Agreement Checklists and TCPs

- Export Control Review Checklist for Agreements
- Export Control Checklist - Subawards
- TCP Standard Template
- TCP Audit Questionnaire

Note: Export Control has various other TCPs [e.g., Substance Control Plan, NDA TCP, CUI TCP/System Security Plan (SSP) etc.].

License Exceptions - Travel Abroad

- TMP License Exception Form
- CCD License Exception Form
- BAG License Exception Form
- Accessing Export Controlled Data While Abroad

Procurement

Purchasing and Export Control provides guidance for processing purchases in accordance with U.S. export regulations.

- ITAR Vendor Certification WITH Registration Template
- ITAR Vendor Certification WITHOUT Registration Template

Employment

- Bona Fide Employee Certification Form (ITAR)
- HR-Payroll Checklist

Restricted Party Screening

- Code of Conduct form

Visitor Logs

- Visitor Logs
- visitor_log_with_dates.doc