University of Arizona Export Control

Beyond the Basics: A Review for the Experienced Researcher

This information is intended to be a quick refresher for researchers with experience and training working with projects secured by a Technology Control Plan (TCP). Please email questions or concerns to export@arizona.edu.

EAR AND ITAR: RED FLAGS

<table>
<tr><th>EAR (Export Administration Regulations)</th><th colspan="3">ITAR (International Traffic in Arms Regulations)</th></tr>
<tr><td>Items that are not ITAR typically are controlled under the EAR.

Dual-Use items - have both a civilian and military application.

EAR 99: Items controlled by Commerce with limited implications to national security but subject to sanctions and embargoes.</td><td colspan="3">Articles and services related to defense and military applications.</td></tr>
<tr><td colspan="4">TYPES OF ITEMS</td></tr>
<tr><td>• Special Materials, Chemicals, Microorganisms, and Toxins
• Electronics
• Computers</td><td>• Telecommunications and Information Security
• Sensors and Lasers
• Navigation and Avionics
• Aerospace and Propulsion</td><td>• Firearms, weaponry, armament
• Launch vehicles, missiles, rockets
• Explosives and propellants
• Toxicological agents & equipment
• Nuclear weapons</td><td>• Military ground, air, or submersible vessels & equipment
• Spacecraft
• Personal protective equipment
• Laser, imaging, guidance equipment
• Directed energy weapons</td></tr>
<tr><td colspan="4">WATCH FOR . . ..</td></tr>
<tr><td colspan="2">Items, data, or information with military, space, and/or national security use or implications.</td><td colspan="2">Commercial items modified:
○ yielding military, space, or national security implications.
○ with ITAR component(s).</td></tr>
<tr><td colspan="4">RESTRICTIONS</td></tr>
<tr><td colspan="2">Some non-US Persons*
Varies country-by country depending on item.</td><td colspan="2">All non-US Persons
*Some rare exemptions</td></tr>
</table>

Take-away: Almost ***everything*** is subject to export control regulations. Determining if an activity or item is subject to EAR or ITAR provides information regarding restrictions for non-US Person involvement or access. These restrictions require either a license or other authorization **BEFORE** involving a non-US Person.

WHY DO I NEED A TCP FOR NDAs/CDAs/PIAs, etc.?

A Technology Control Plan (TCP) is necessary to document required protections before any data, source code, or information that is subject to export control regulations is exchanged in discussions related to a potential research project.

Take-away: Ask the other party to identify and mark any export-controlled data that will be provided. If a TCP is not in place, contact Export Control before accepting anything from the potential partner.

EXPORT-CONTROLLED DATA

Data subject to export regulations can be in tangible or intangible form, such as written or oral communications, blueprints, engineering designs and specifications, or revealed through visual inspection of an item. These include plans, diagrams, models, formulae, tables, manuals, drawings, photographs, computer-aided design files, instructions. This also includes information necessary for:

Design Development Production	Maintenance Modification Testing	Manufacture Overhaul Refurbishing	Installation Repair Use	Operation Assembly Software related to defense articles

EXPORT-CONTROLLED DATA: EMAILING & CLOUD STORAGE

- Must be encrypted end-to-end.
- Use FIPS 140-2 or AES 258 encryption strength.
- Determine locations of cloud storage servers. Data cannot be sent or stored in the Russian Federation or a country subject to U.S. arms embargoes (which includes the People's Republic of China, among other countries).
- Remember, Controlled Unclassified Information (CUI) cannot be emailed.

CONSULT WITH EXPORT CONTROL BEFORE THESE ACTIVITIES:

Unless the item is identified by Export Control as EAR99 AND does not involve countries or entities subject to sanctions or embargoes.

- ✓ **Shipping or Transporting** to a Foreign Person/entity in the U.S. or to anyone abroad.
- ✓ **Traveling abroad** while on a TCP.
- ✓ **Accessing** data (whether via email, VPN, flash drive, etc.) abroad.
- ✓ **Using other facilities** (on and off-campus).
- ✓ **Permitting visitors** into an area with export-controlled activities or data.
- ✓ **Assisting** on behalf of/for the benefit of a foreign person/entity/government ANYWHERE. Training, services, support with items or to foreign government (particularly military) end users are likely subject to restrictions.
- ✓ **Transmitting, releasing, sharing** export-controlled items, data, software, or source code in U.S. or abroad, including:
  - **Visual or other inspection** by foreign persons which reveals technical data or technology/source code.
  - **Oral or written exchanges** with foreign persons of data/technology or source code.
  - **Providing access information** (e.g. password), to a database containing data, technology, or source code.

Take-aways: 1. Keep in mind exports may occur via email, video conference calls, conference presentations, casual encounters and discussions, as well as shipping an item or taking or accessing data abroad.

2. Unless a visual or other inspection of ITAR/EAR items "releases" technical data (ITAR) or technology or source code (EAR), the mere presence of a foreign person on the room is not recommended, but would not be an export violation.