Export Controls & Research Security

Lacy Kitchin
Export Control Officer / Facility Security Officer

UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

What is an export?
Export ≠ Shipping

- Physical shipments of tangible goods or items

- Digital transmission/transfer of data, information, or assistance

  - Outside of the U.S. (including to U.S. citizens)

  - To a Foreign National inside the U.S. (deemed export)

  - Release of technology, software, or source code

- Verbal, visual, and written disclosures

What are export controls?

- Export controls are rules that restrict access to certain items, technologies, and information.

- An "export" includes not only physical shipments but also sharing data with certain individuals—even within the U.S.

- Foreign Nationals (non-U.S. citizens or residents) may not access controlled data without authorization.

- **Controlled data may require a license from federal agencies before sharing.**

Key Agencies and Regulations

Bureau of Industry and Security (BIS): governing the export and reexport of commodities, software, and technology (collectively "items") falling under the jurisdiction of the Export Administration Regulations (EAR). "Dual-use" items for commercial and military purposes.

Note: BIS license reviews have been periodically suspended without notice.

Office of Foreign Asset Control (OFAC): Enforces sanctions and embargoes.

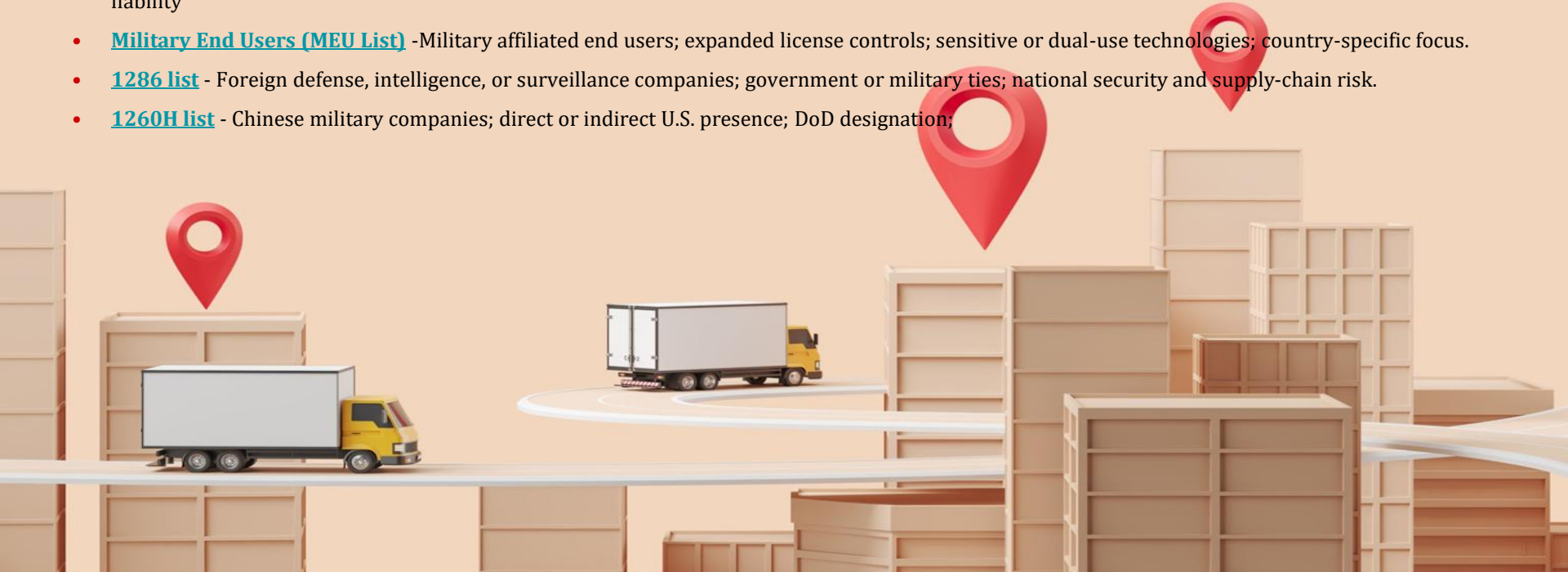**International Traffic in Arms Regulations (ITAR):** Governs military-related exports.

Department of Justice (DOJ): Focuses on U.S. Government Data, Bulk data rules (geolocation, omics, etc.)

Restricted Parties & Prohibited Entities

Federal regulations strictly prohibit interactions with certain restricted parties and can implement a "policy of denial" or immediate suspension of license requests to ensure national security.

- **BIS Entity List** - Restricted foreign parties; presumption of denial; specific license requirement; national security or foreign policy risk.

- **BIS Unverified List** -Inability to verify end use or end user; heightened due diligence; mandatory customer statements; shipment risk factor.

- **OFAC SDN List (Specially Designated Nationals)** -Sanctioned individuals and entities; asset blocking; U.S. person prohibited from transactions; strict liability

- **Military End Users (MEU List)** -Military affiliated end users; expanded license controls; sensitive or dual-use technologies; country-specific focus.

- **1286 list** - Foreign defense, intelligence, or surveillance companies; government or military ties; national security and supply-chain risk.

- **1260H list** - Chinese military companies; direct or indirect U.S. presence; DoD designation;

Travel

- All international travel is screened for potential export control issues.

- If you are traveling internationally with any university-owned equipment (including laptops, cell phones, or iPads), you must complete the **Export Control Travel Checklist** before traveling.

- Please complete the form **at least two (2) weeks prior to travel**.

- If you intend to take equipment that requires a license, please allow time for processing. Laptops, etc. must be "Hand Carried" in your carry-on or checked luggage.

- Sanctioned countries or countries of concern may require additional screening and/or licensing to travel with equipment. (Cuba, Iran, Syria, North Korea, Venezuela)

Conferences and Presentations

- Conferences should be open to the public.

- Only present information that is public knowledge, published, or intended to be published.

- Do <u>not</u> present any unpublished or sensitive data.

- Additional controls may apply to countries of concern and research in areas of new and emerging technology.

- Prior to travel, you may be asked to submit a copy of your presentation to screen for potential export control concerns.

- Remove all sensitive information (CUI, UCNI, Omics, Govt. Data) from your devices before travel.

Other Activities Reviewed by Export Control and Research Security

- Foreign Collaborations
  - IP protection, hosting international visitors, risk assessments
- Foreign Talent Recruitment Programs
  - Position/activity that includes compensation, honorifics, career advancement, etc. directly provided by a foreign country at any level, either directly or indirectly.
- Insider Threats
  - Espionage, theft, sabotage, workplace violence, or other harm to people and organizations
- Persistent Identifiers
  - A long-lasting reference to a digital resource. (ORCID)
- Undue Foreign Influence
- Research Security Training

Secure enclave Research Environment (SeRE)

⚠ **High-Cost Resource:** The SeRE is a highly specialized environment. Due to significant infrastructure costs, it is strictly reserved for data that legally requires this level of protection.

ELIGIBILITY CRITERIA: NIST 800-171

Access is granted only for research involving Controlled Unclassified Information (CUI) that mandates adherence to NIST 800-171 security standards. This includes specific controls for access, audit, and incident response.

Restricted Third-Party Data: Proprietary industry data with contractual security mandates beyond standard university systems.

ELIGIBLE DATA EXAMPLES

NIH DbGaP Data: Specific genomic datasets designated as "controlled access" which contain sensitive individual-level human data.

Export Controlled Data: Technical data under ITAR (International Traffic in Arms Regulations) or EAR (Export Administration Regulations).

Questions or Assistance?

- Some activities are prohibited—contact Research Security staff for guidance.

- Visit the Export Control and Research Security websites for more information.

- **Contacts:**

- Export Control & Research Security: exportcontrol@charlotte.edu

  - Export Control Officer / FSO: Lacy Kitchin (704) 687-1877; lkitchin@charlotte.edu

- **Links:**

- Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (Bulk Data Regulations)

- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST 800-171 standards and controls)

- Supplement No. 3 to Part 732, Title 15 -- BIS's "Know Your Customer Guidance and Red Flags" - eCFR