USC University of Southern California

It's Fundamental!
Managing Export Controls at USC

March 29, 2017

Agenda

- Recap of Export Control regulations
- Export Control "safe harbors"
- Export Control "red flags"
- IT Security practices
- Questions

What Are Export Control Laws?

U.S. laws that regulate :

- the distribution of technologies, equipment, hardware and software, and
- the provision of technical assistance to foreign nationals, foreign countries and listed individuals & entities

AND U.S. laws that regulate :

- payments and services to sanctioned individuals, entities and comprehensively sanctioned countries for reasons of foreign policy and national security.

What is an Export?

- Physical Export: Sending, transferring or taking a tangible item outside of the U.S.
- Deemed Export: Disclosing (including oral or visual disclosure) technical data, technology, or source code to a non-U.S. Person, in the U.S. or abroad
- Defense Service: Providing technical assistance, training, or defense services to a non-U.S. Person, whether in the United States or abroad

22 CFR §120.17 and 15 CFR § 734.2

Export Control Regulations

*Research subject to contract restrictions on publication or access by foreigners

*Research conducted outside the U.S.

*Research in space, nuclear technology, or Weapons of Mass Destruction

*Research in certain encryption technology

*Research in chemical/biological weapons

*Research with 3rd party Controlled technology

*Interactions with blocked or sanctioned entities

*The activities above may need Export Control Review

<u>Fundamental Research</u>

<u>Public Information</u>

<u>Educational Information</u>

Structure of the Regulations

***Commerce Department*: Bureau of Industry and Security (BIS)**

Export Administration Regulations (EAR)

“dual use / commercial”

***State Department*: Directorate of Defense Trade Controls (DDTC)**

International Traffic in Arms Regulations (ITAR)

military

Treasury Department: Office of Foreign Assets Control (OFAC)

Economic sanctions (countries, entities, individuals)

All items

Department of Energy (DOE) and \Nuclear Regulatory Commission (NRC)

Part 810 and Part 110 Regulations

nuclear fuel cycle, equipment, technical data

ITAR Examples

- **Launch vehicles, missiles, rockets**
- **Military spacecraft and UAVs**
- Military aircraft and vehicles

- Military training and simulation articles
- Military electronics, night vision, infrared cameras, inertial measurement units, navigation systems
- Toxicological agents, including chemical and biological agents, and associated equipment

EAR: Export Classifications

- CCL has ten categories, including:
  - 0: Nuclear Materials, Facilities and Misc.
  - 1: Materials, Chemicals and Toxins
  - 2: Materials Processing
  - 3: Electronics
  - 4: Computers
  - 5: Telecommunications and Information Security (encryption)
  - 6: Sensors and Lasers
  - 7: Navigation and Avionics
  - 8: Marine
  - 9: **Propulsion Systems, Space Vehicles and Related Equipment**

How does this impact universities?

- Export controls and sanctions regulations may restrict the University's ability to:
  – Export hardware, software, technology and services from the U.S.
  – Include foreign national faculty and students in research within U.S.
  – Collaborate with foreign researchers and institutions
  – Engage in corporate and government sponsored research projects
  – Travel to certain countries
- U.S. enforcement agencies are increasingly focused on universities and their compliance issues

USC Safe Harbors: The "Fundamental Research" Exclusion (FRE)

- Information **arising during or resulting from:**
  – Basic and applied research in science and engineering
  – When the resulting information is ordinarily published and shared broadly in the scientific community
- Covers **most** research at USC.

FRE Generally Does NOT Apply If

- The PI intends to withhold some research results from publication for proprietary use.
- The university accepts any contract clause that
  - Forbids / restricts the participation of foreign persons
  - Gives the sponsor a right to approve/restrict publications resulting from the research, except for limited IP protection
  - Restricts access to and disclosure of research results
  - Allows for performance of the research outside the United States.
- But for U.S.-Government funded research, some access and dissemination controls are acceptable

USC "Red Flags"

- As a general rule, University activity is not subject to export controls.
- The challenge lies in catching what is, or what could be.
- **Theme**: Information intended to be shared or that is already in the public domain does not raise export control considerations.
- The "red flags" that follow, however, require consideration of export control requirements.

“Red Flag” #1: *Contractual restrictions on personnel or publication*

- USC attempts to negotiate out these restrictions whenever possible.
- If we accept, USC ensures compliance by:
  - Limiting foreign nationals/students or obtaining license
  - Implementing technology control plans (TCP’s) if restricted “input” data will be provided or restricted “output” data will be generated
  - Monitor compliance on an ongoing basis throughout the life of the project.

Your Role:
- If a sponsor informs you or you become aware of contractual restrictions, notify the Office of Compliance
- Comply with any and all contractual restrictions agreed to as part of the project as well as USC measures.

“Red Flag” #2: *Receipt of proprietary/export controlled data (sponsor provided, NDA, MTA)*

- USC requires sponsor notification and the right to decline to receive such data.
- For third party data providers, USC screens all incoming NDA’s/MTA’s and requires explicit notification when proprietary/export-controlled data is to be provided.
- When we accept, we ensure compliance much the same way we do on personnel/publication restrictions. Case-by-case analysis.

Your Role:
- Provide thorough description of data to be provided when known to enable export assessment
- Comply with all contractual restrictions as well as USC measures.

"Red Flag" #3: *Prototype/software development*

Generally, releases of technology necessary for the "development", "production" or "use" of an item are subject to export control regulations.

- "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, and layouts.
- "Production": Related to all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance.
- "Use": Information related to the operation, installation, maintenance, repair, overhaul, or refurbishing of the item

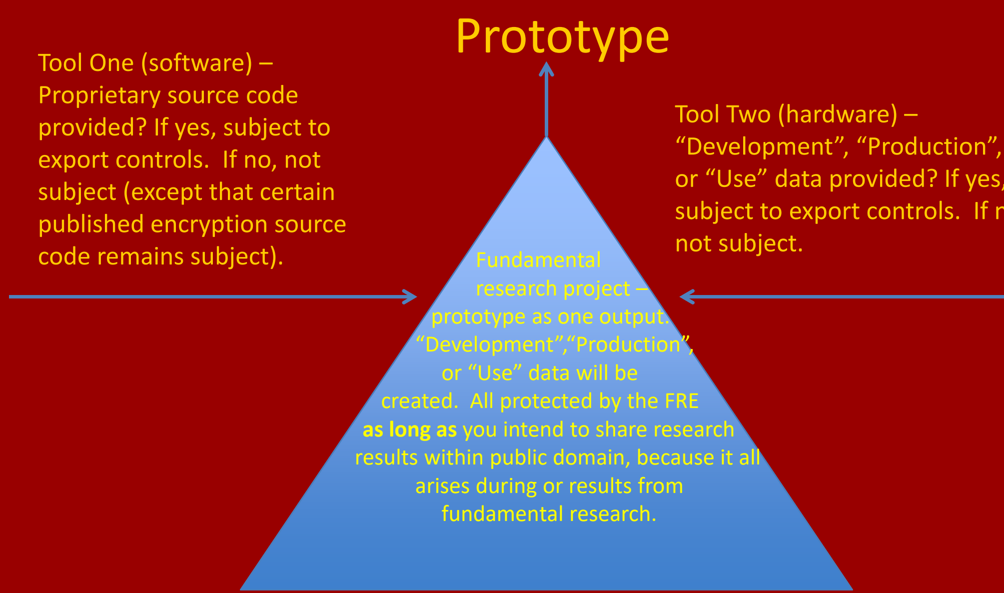
"Red Flag" #3 (Con't.): *Prototype/ Software development*

- **FRE = important safe harbor.**
- If you are conducting fundamental research giving rise to a prototype, technology related to its "development", "production" or "use", and associated software/software source code, is not export controlled.
- If, however, you are using third party technology or items as tools to conduct your research (which may include a prototype as output), such items do not "arise during or result from" your fundamental research. If you are provided technology regarding the "development", "production", or "use" of such technology or items, or software source code, this information is subject to export controls, **even though** your research output is fundamental.

Your Role:

- If you are developing a prototype or software, your intent should be to share it broadly into the public domain on your fundamental research projects.
- If you obtain items, components, or software from third parties that you are using as tools or components of a prototype **and** will receive "development", "production", or "use" data, or software source code, notify the Office of Compliance so that an export assessment can be performed.

“Red Flag” #3 (Con’t.): *Prototype/Software development*



“Red Flag” #4: *Certain uses of equipment to perform research*

- Equipment is routinely used in USC research, and on projects that do not contemplate a prototype. Few of these uses are subject to export controls.
- However, under export regulations, certain “uses” of equipment are controlled if **all** six elements of use are present:
  – Operation
  – Installation
  – Maintenance
  – Repair
  – Overhaul
  – Refurbishing

Your Role:

- If you have foreign nationals using equipment in the manner described above, notify the Office of Compliance
- There are certain license exemptions that may apply, but that require signed assurances and monitoring.

"Red Flag" #4: *Certain uses of equipment to perform research*

Some types of equipment are more controlled than others, and subject to greater scrutiny under export regulations. These include:

- Infrared cameras, night vision equipment and lasers
- Inertial measurement units
- UAVs and satellites
- High performance computers and integrated circuits
- Chemical and biological agents

"Red Flag" #5: *Actual Exports*

- The Fundamental Research Exclusion applies only to information arising out of research performed in the United States.
- It does not apply to **any** actual export (e.g., shipping items abroad, taking items abroad with you on international travel, licenses of technology to foreign business partners).
- **All** actual exports require an export analysis.
- USC will obtain all necessary licenses or authorizations. However, if the need for a license does not arise out of USC research activity (e.g., a license to a foreign partner who will perform its own research or use for commercial purposes), the cost of obtaining this authorization is borne by the customer, not USC.

Your Role:

- Enlist the Office of Compliance as early as possible when you know of a possible actual export.

“Red Flag” #7: *International Travel*

While USC encourages international travel, a variety of legal issues can arise depending on:

- Where you are going
- What you intend to take with you
- Who you will be working with on your trip
- The nature of the information you take with you

“Red Flag” #7 (con’t.): *International Travel*

- Where you are going:
  - Travel Warnings issued by State Department
  - Economic sanctions under OFAC (if applicable)
  - Enrollment in State Department “STEP” program
  - CDC warnings
- What you are taking with you:
  - Laptops are OK, so long as no special encryption technology
  - Taking any export controlled or otherwise restricted information you have on your laptop **is an export.**
- Who you will be working with:
  - Collaborations on fundamental research projects are fine.
  - Payments to foreign governmental officials are prohibited under the FCPA.
  - Collaborations on restricted projects require review and possible export authorization.
- Protecting information you take:
  - Do not take sensitive data if at all possible.
  - Adhere to international travel checklist and its IT Security recommendations.
  - http://ooc.usc.edu/sites/ooc.usc.edu/files/pdfs/International-Travel-Checklist_7-31-14.pdf

Red Flag #8: Foreign National Visits, Collaborations, Sales

- You need to know who is on the other end of the phone, email, collaboration, visit – Conduct Restricted Party Screening (RPS).
  - RPS determines if the individuals and companies with whom you engage are on any government issued restricted, blocked, or denied party lists. Request a restricted party screening from the Office of Compliance for entities and individuals prior to engagement (e.g. collaboration, visit).
- Screen all visitors, institutions, and companies prior to visit, travel, collaboration, etc.

Behind the Scenes

- International Collaborations policy: addresses export controls, OFAC and international travel, and FCPA to be issued in Fall -16
- Screening process for H1-B workers and J-1 visiting scholars
- Assist in performing OFAC analyses for international travel, particularly for more sensitive/restricted locations like China, Iran, and other countries in the Middle East.
- Educate international staff regarding FCPA obligations
- Engage in ad-hoc monitoring of usage of hi-risk equipment
- Assist in instances involving actual export
- Continue to monitor projects with publication/personnel restrictions
- Implement Technology Control Plans (TCP) in instances involving input/output restrictions for security sensitive/export control purposes
- Monitor incoming NDA's/MTA's to identify instances where export-controlled items or information are to be provided
- Coordinate with IT security stakeholders to meet onerous security standards. (DFARS 252.204-7012).

Questions

Daniel Shapiro
Director, Research Compliance
dshapiro@ooc.usc.edu
(213) 740-8258