Handling Export-Controlled Information

This table identifies key project components that render an activity subject

	Subject to Export Control?
Public domain, and: • No equipment, encrypted software, listed-controlled chemicals, bio-agents or toxins, or other restricted technologies are involved, and • Information/software is already published, and ➢ There is no contractual restriction on export, or ➢ Project consists of Fundamental Research (note definitions and caveats associated with this exemption).	NO
Equipment or encrypted software is involved, or: • Technology is not in the public domain, and • Technology may be exposed to foreign nationals (even on campus) or foreign travel is involved, and ➢ The equipment, software or technology is on the Commerce Control List, or ➢ Information or instruction is provided about software, technology or equipment on the CCL, or ➢ The foreign nationals are from or the travel is to an embargoed country, or ➢ The contract has terms e.g. a publication restriction that affects the Fundamental Research Exclusion.	Probably. Further review is required. License may be required.
➢ Equipment, software, chemical, bio-agent, or technology is on the U.S. Munitions List (ITAR), or ➢ Equipment, software, chemical, bio-agent or technology is designed or modified for military use, use in outer space, or there is reason to know it will be used for or in weapons of mass destruction, or ➢ Chemicals, bio-agents or toxins on the Commerce Control List are involved, or ➢ The contract contains a restriction on export or access by foreign nationals.	Yes. License will be required.

Adapted from: https://uh.edu/research/compliance/export-controls/do-ec-apply/

When a sponsored research project is subject to export controls a Technology Control Plan (TCP) must be done. The TCP will outline the procedures to be taken to handle and safeguard the export-controlled information. It is the responsibility of the Principal Investigator (PI) to develop a written TCP which must be approved and signed by the Executive Director of Sponsored Programs, in consultation with the UH Research Integrity and Oversight (RIO) Office. A copy of the plan will be kept with the award folder. The PI must ensure each person working on the project has read and understands the TCP and the briefing below on the handling of export-controlled information on research projects.

Briefing

In general, export-controlled information means activities, items, and information related 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 utility. Export-controlled information does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of export-controlled information is military or civil in nature.

Technical information, data, materials, software, or hardware (i.e. technology generated from this project) must be secured from use and observation by unlicensed non-U.S. citizens. Security measures will be appropriate to the classification involved. Examples of security measures are:

- Project Personnel - Authorized personnel must be clearly identified.
- Laboratory “work-in-progress” - Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
- Marking of Export-Controlled Information - Export-controlled information must be clearly identified and marked as export-controlled.
- Work Products - Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; located in rooms with key-controlled access.
- Equipment or internal components - Such tangible items and associated operating manuals and schematic diagrams containing identified “export-controlled” technology are to be physically secured from unauthorized access.
- Electronic communications and databases - Appropriate measures will be taken to secure controlled electronic information. Such measures may include user ID, password control, SSL or other approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.
- Conversations - Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

Adapted from https://uh.edu/research/compliance/export-controls/handling-ec-info/