EXPORT-CONTROLLED INFORMATION, ITEMS, TECHNOLOGY AND SOFTWARE
Information for Principal Investigators

This project/activity involves the use of export-controlled information (including technical data), item, technology, or software. As a result, the project/activity falls under either the International Traffic in Arms Regulations (ITAR) administered by the Department of State, or the Export Administration Regulations (EAR) administered by the Department of Commerce.

It is unlawful to send or take export-controlled information, item, technology, or software out of the U.S. without authorization. In addition, it is unlawful to release export-controlled information, technology, or software to a foreign person inside the U.S. without proper authorization. A license may be required for foreign nationals to access export-controlled information, item, technology, or software. A foreign national is a person who is not a U.S. citizen, U.S. permanent resident, or a person who is protected under the U.S. refugee and asylum status. The law makes no exceptions for foreign graduate students.

In general, export-controlled information means information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. It also includes information necessary for "production", "development", and "use" of controlled commercial items and items for dual-use purpose (i.e. items with both civil and military application).

Information generated from, or related to this project must be secured from use and observation by unauthorized foreign nationals. Security measures will be commensurate with the export classification of information and items 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; preferably 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.

Each project subject to export controls must have a Technology Control Plan (TCP) that outlines the procedures to be taken to handle and safeguard the export-controlled information, item, technology or software. Please contact the University Research Compliance Office (URCO) for assistance with developing the TCP – comply@ksu.edu; phone 785-532-3224.