Foreign Travel With Export Controlled Materials

Before traveling with or transporting certain, potentially export-controlled materials abroad, the traveler must complete an eShipper form and receive approval from Export Controls. Once the traveler receives an approval confirmation e-mail from Export Controls, it is the traveler's responsibility to forward the confirmation to Travel at Travel@SLAC. For foreign travel involving potentially export-controlled materials, receiving an approval confirmation on a filed eShipper form is a prerequisite to travel being approved.

Potentially export-controlled items that require approval include, but are not limited to:

1. Transporting any physical items such as scientific instrument(s), tool(s), sample(s), prototypes, raw materials, or other such items by either checked baggage or carry-on.

2. Shipping and/or mailing any physical items such as scientific instrument(s), tool(s), sample(s), prototypes, raw materials, or other such items related to the individual’s travel plan(s).

3. Proprietary data or software, in whatever format, such as information or data whose release is limited by:
   a. Non-disclosure or confidentiality agreements
   b. Government restrictions or markings (classified, OUO, SBU, HIPAA, etc.)
   c. Intellectual property protection consideration
   d. Non-ODD software and trade secrets

4. Any personal, University, or Government Furnished laptop(s), mobile phones, mobile Wi-Fi hotspots, memory cards, external drives, thumb drives, or other hand-held computer or communication device(s) onto which export controlled technical data is stored including:
   a. Export controlled research or export controlled contract;
   b. Controlled, proprietary data received under an Non-Disclosure Agreement (NDA) or other confidentiality agreement; or
   c. Proprietary vendor materials (e.g. manuals or materials) identified as export controlled

   (Technical data does not include the results of fundamental research programs to which no publication, citizenship or dissemination restrictions apply)

5. Any personal, University or Government Furnished laptop(s), mobile phones, mobile Wi-Fi hotspots, memory cards, external drives, thumb drives, or other hand-held computer or communication device(s) that contains specialized dual-use software other than operational software normally embedded in your laptop or hand-held communication devices such as Microsoft Office, Microsoft Edge, Internet Explorer, Adobe, FireFox, etc.

6. Any personal, University, or Government Furnished laptop(s), mobile phones, mobile Wi-Fi hotspots, memory cards, external drives, thumb drives, or other hand-held computer or communication device(s) onto which export controlled cryptography or cryptographic functionality is stored including any advanced or specifically designed cryptography, or any cryptographic programs specifically identified by a vendor or licensor as export control.
Traveling With Government Furnished Equipment

All Government Furnished Equipment (GFE) must remain within the physical custody of the traveler at all times during travel except when visiting a secure foreign facility. All GFE items are not to be entrusted to the care of custodianship of foreign nationals/governments or any individuals (i.e. airport customs officer, hotel bellman, taxi driver, flight attendant, etc.), stored in remote locations (i.e. gym or airport storage locker, checked baggage in the airplane cargo, hotel room or safe, rental car, etc.) or removed from the traveler to whom issued.

GFE items may not be connected to open public networks, unauthorized devices, or unsecured Ethernet connections to remotely access the DOE networks and applications. To remotely access DOE networks and application, the traveler must do the following:

1. Remote access must be secured through multi-factor authentication including the use of RSA SecureID Tokens and Personal Identification Verification cards to access DOE resources, networks, and applications.

2. Secure remote access on GFE devices may only be conducted through a Citrix Receiver, Virtual Private Networks (VPN) or Virtual Desktop Interface (VDI), secured Ethernet or Wi-Fi connection, or connection to a GFE Mi-Fi device.

Devices received from foreign nationals/governments or devices purchased while on foreign travel may not be used to conduct official DOE business.

Tips For Foreign Travel with Export Controlled Materials:

1. Travelers are responsible for being aware of a foreign country’s import control. Travelers may be responsible for duties or taxes if they do not have proper documentation when entering customs. To check, please click here: https://commons.lbl.gov/display/~ewalker@lbl.gov/Foreign+Travel+Information.

2. Travelers may not bring back any export controlled items that they did not originally take upon departure from the United States or have prior approval to take with them.

3. Travelers should take precautionary measures when handling, using, or transporting export controlled items and/or DOE GFE such as:
   a. Terminate all session connections when not in use
   b. Limit web browsing and access to social media, and refrain from using non-DOE managed web and storage services while abroad
   c. Beware of eavesdropping and shoulder-surfing, particularly in public spaces and modes of transportation (i.e. trains, buses, etc.)
   d. Be vigilant of technical eavesdropping or the use of audio or video devices to record your actions and information

Violations and Consequences:

It is the traveler’s responsibility to abide by export control requirements to avoid potential loss of proprietary information or technology. Penalties for export violations range from thousands to millions of dollars per violation. Travelers who violate export control requirements may also be subject to criminal penalties up to serving time in federal prison.