

All UA faculty and staff traveling overseas for University business or meetings should contact the Export Control Officer (ECO). Send a travel advisory request (attached) to the ECO's office at least two weeks prior to leaving the country.

Information needed:

- Destination(s)
- Exact travel dates
- Nature of your visit
- Who you will be meeting with (names, business or university affiliations with addresses)
- What you will be discussing
- Is the travel associated with a specific contract (need FRS no. and title)
- Is the project export-controlled?
- Is there an export authorization in place (need license or TAA number)
- List of software on your laptop
- Is there encryption software on your devices (some countries restrict the import of encryption software)

Depending on your international destination(s), an export license or other government approval may be required for your laptop computer, software, or other equipment. Laptops, Blackberrys and other PDAs are export-controlled by the DoC but may be hand-carried under the exception for temporary exports – tools of the trade (TMP). Tools of trade must remain under the “effective control” of the exporter, meaning in your physical possession or secured in a hotel safe. TMP exceptions depend on the equipment and the country of your destination. Encryption software in particular is subject to special regulations and more stringent license requirements.

Presentations and discussions must be limited to topics that are not related to controlled items or technologies unless that information is already published or otherwise already in the public domain. Verify that your technology or information falls into one or more of the following categories prior to traveling:

- Research that qualifies for the fundamental research exclusion
- Published information

- Publicly available software
- Educational information
- Patent applications

We strongly recommend that you do not take your UA laptop with you on your international travels, but if you decide to, there are some guidelines to follow:

- Remove export-controlled information, technical data, and software from your laptop or thumb drive prior to leaving the United States
- Use a “shredder” program to erase the information you do not want to share so that it cannot be recovered
- Encrypt and then e-mail to yourself any information you may need while overseas. Do not retrieve the e-mail until you have reached your destination, and remember you will need to remove it completely prior to returning to the U.S. or prior to crossing any international border.