



Foreign Travel with Computers and Other Electronic Devices

Quick summary: In most cases if you're traveling to another country with a university-owned laptop with typical office productivity software, you will probably not need an export license as long as the equipment is always under your immediate control and returns to the US. If the travel involves an embargoed country, or you have non-retail-grade encryption software installed, or the laptop includes EAR- or ITAR-controlled technical data, or the hardware is unusually sophisticated, you should check with the Office of Regulatory Compliance (303-724-1010) for further advice.

If you will be temporarily traveling (less than one year) outside of the United States, you may take with you for activities related to your travel laptop computers, other portable computing devices, data storage devices and other equipment that people in your discipline would generally recognize as tools of trade as long as you maintain **effective control** of those items while you are outside of this country **AND** you are not traveling to an embargoed country (for current list, check: <http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>). You maintain effective control over an item when you either retain physical possession of the item or you secure the item in such an environment as a hotel safe, a bonded warehouse, or a locked or guarded meeting or conference facility.

Maintaining *effective control* of the items and the limit of one year do not apply if **ALL** of the following apply:

- The laptops and other computing and data storage devices are standard, off-the-shelf products that are broadly available; and
- The operating system and any encryption capabilities are of the kind that are preloaded on the computers and do not allow for user revisions to enhance communications security capabilities; and
- All of the application programs are general, commercially available software that either do not perform technical analyses; or, are general purpose scientific or engineering programs that are commercially available (e.g., for electric field calculations not aimed at a specific product); and
- All of the data stored on the computers or storage devices is publicly available (e.g., published in journals or on the web). Data and analyses from research that ordinarily would be published and are not restricted by contract from general dissemination can be treated as publicly available; and
- The travel is not to a country with special strong export controls, currently Cuba, Iran, Iraq, North Korea, Syria or Sudan; and
- You have no reason to believe that there are export constraints on any of the equipment, software, data or information that would apply to your intended travel.

There are many other devices and equipment for which there are minimal constraints under the export rules. If you have an issue with regard to maintaining effective control over an item, you might check with the people identified in the first paragraph above.

You should not take with you ANY of the following without first obtaining specific advice from the Office of Regulatory Compliance at 303-724-1010 or reg.compliance@ucdenver.edu.

- Data or information received under an obligation of confidentiality.
- Data or analyses that result from a project for which there are contractual constraints on the dissemination of the research results.
- Computer software received with restrictions on export to or on access by foreign nationals.
- Devices or equipment received with restrictions on export to or on access by foreign nationals.
- Private information about research subjects
- Devices, systems or software that was specifically designed or modified for military or space applications.
- Classified information

Traveling outside the US with laptops, PDAs, cell phones or storage devices involves special considerations and may require an export license. US export laws may involve:

- Hardware. Generally speaking, computer hardware is not subject to tight restrictions, though there are limitations on “high performance” computers exported to embargoed countries.*
- Software. US export laws impose significant restrictions on encryption software. Public domain software is often already licensed for export—this can be confirmed by checking with the vendor (e.g., www.microsoft.com/exporting/). Non-commercial encryption software in source code or object code is particularly likely to be restricted; please check with the Office of Regulatory Compliance (303-724-1010) if you have questions.
- Controlled data. If you are working on a project that involves EAR or ITAR controlled technologies, your laptop may contain controlled technical data that may not be shared with foreign parties without a license. It is critical that you inform the Office of Regulatory Compliance if such data may have been compromised while traveling due to the device being lost, stolen, or outside your control.

If the computer or other equipment is owned by the University of Colorado, the equipment as well as any installed encryption software may be eligible for License Exception TMP (Temporary Exports). To qualify for this exception, the equipment:

- Must be a “tool of the trade”
- Must remain under your “effective control” while overseas. This means that it must remain in your personal possession or in a locked hotel safe (a locked hotel room is not sufficient) at all times.
- Must be returned to the US (or destroyed) within 12 months.
- May not be taken to embargoed countries*

If you personally own the equipment, it may qualify for License Exception BAG (Baggage). To qualify for this exception, the equipment and retail-level encryption software must be for your personal use in private or professional activities. “Strong” encryption software may also qualify for this exception, unless the travel (or traveler) involves embargoed countries*.

Beyond export laws, you should also be aware that traveling with electronic devices may result in unexpected disclosure of personal information. Certain countries are noted for accessing files upon entry, so you should be extremely careful about any proprietary, patentable, or sensitive information that may be stored on your device. (For certain countries, this includes material that might be

perceived as pornographic, or culturally inappropriate.) Homeland Security personnel may also decide to inspect your laptop upon return to the US, in which case everything on the device is subject to inspection. You should be wary about including on a laptop that you take overseas any financial or other personal information that you would not want viewed without your permission.

If your university-owned laptop contains controlled software or sensitive data—particularly data that may be controlled under ITAR or EAR regulations—you might consider alternatives. For example, if the laptop is to be used only for making presentations, can you use a memory stick instead? If you are using the laptop for other purposes (such as email), can you instead take a “clean” computer that does not include the restricted software, data, or other sensitive information?

You should keep in mind and be prepared for the potential that customs inspectors in countries that you may visit, and in the United States when you return, may require that you allow them access to inspect the devices and equipment you have with you and all of the contents of the computers and storage devices. In the United States, the inspectors may take possession of those items for various periods of time, and even permanently depending upon the circumstances. The inspectors in other countries might do so as well.

The following are some examples:

You plan to travel to France to do research on early French literature and would take a laptop computer and flash memory storage device with you. It is very likely that the export regulations would not require that you maintain effective control of the computer and memory, according to the guidance given above.

You plan to travel to Japan to present a paper on the latest results of your research on a basic issue of physics. You plan to take a laptop computer and copies of some published papers with you. You do not have any information or computer software that was received under an obligation of confidentiality or a need to exclude the use of the software by foreign nationals. It is very likely that the export regulations would not require that you maintain effective control of the computer and memory, according to the guidance given above.

You are planning to travel to Brazil to study some ancient ruins. You would like to take with you a laptop computer, a portable storage device, standard surveying equipment that is easily available throughout the world, and a PDA with GPS capabilities. You might need to maintain effective control over the PDA. If you do not feel you can maintain effective control, you should seek advice as noted above.

You plan to bring a number of smart sensors to Australia for use in a research project to monitor stresses in a structure. Each smart sensor includes an acceleration sensor, a relatively low speed microprocessor and a low speed wireless communications capability. You would also take a laptop computer with communications capabilities to interact with the smart sensors. The export regulations likely would not require that you maintain effective control over them; but you should seek advice as noted in the first paragraph above in case there is an issue. You should not take with you any information or computer software received under an obligation of confidentiality or with restrictions on access by foreign nationals.

If you have questions, please check with the Office of Regulatory Compliance at 303-724-1010; reg.compliance@ucdenver.edu.