Foreign Travel with Computers & Other Electronic Devices

Most foreign travel with a university-owned laptop with standard software will not require an export license. However, you should always keep such items under your immediate control and return them to the U.S. within a year. If you are traveling to an embargoed country*, or you have non-retail grade encryption software installed on your device, the device includes EAR or ITAR controlled technical data, or the hardware is unusually sophisticated, you should check with the Office of Research Integrity (Bridget Watson, 907-474-7832 or bjwatson@alaska.edu).

Traveling outside the U.S. with laptops, tablets, smart phones or storage devices involves special considerations and may require an export license:

- **Hardware**. In general, most laptops are not subject to restrictions, as long as you return them to the U.S. within a year. However, there are limitations on "high performance" computers exported to embargoed countries.*
- **Software**. Most commercial and public domain software is often already licensed for export—this can be confirmed by checking with the vendor (e.g., https://www.microsoft.com/en-us/exporting). The most significant restrictions apply to encryption software. Commercially-available software can be installed on devices that otherwise qualify for the license exceptions listed below. Non-commercial encryption software in source code or object code is likely to be restricted; please check with the Office of Research Integrity (907-474-7832) if you have questions.
- **Controlled data**. If you are working on a project that involves EAR or ITAR controlled data or technology, your device may contain controlled technical data that cannot be shared with a foreign national unless you have an export license. **It is strongly recommended that you not take such data outside the U.S.** If you do, it is critical that you inform the Office of Research Integrity if your device is or may have been compromised (device is lost, stolen, or outside your control) while traveling.

If the computer or device is owned by UAF, it as well as any pre-loaded encryption software may qualify for License Exception "TMP" (Temporary Exports). To qualify, the equipment:

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

If the device is your personal property, it may qualify for License Exception "BAG" (Baggage). To qualify for this exception, the device and pre-loaded 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 activities involve an embargoed country*.

You should not take with you ANY of the following without first obtaining specific advice:

- Data or information received under an obligation of confidentiality or is otherwise classified.

- 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 human research subjects
- Devices, systems or software that was specifically designed or modified for military or space applications.

Beyond export laws, you should also be aware that traveling with electronic devices may result in unexpected disclosure of personal information. Certain countries are known 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. Homeland Security may also decide to inspect your laptop upon return to the U.S., in which case everything on the device is subject to inspection. In the U.S., the inspectors may take possession of such items for various periods of time, and even permanently depending upon the circumstances. Inspectors in other countries may do so as well. You should be wary about having any financial or other personal information that you would not want viewed without your permission on a laptop that you take overseas.

If your UAF-owned device contains controlled software or sensitive data, particularly data that may be controlled under ITAR or EAR regulations, we strongly recommend that you do not travel with it, especially internationally. If a laptop will only be used to give a presentation, consider taking a thumb drive or storing the presentation on a cloud-based server instead. If you are using a laptop for other purposes (such as email), consider taking a "clean" laptop that does not include the restricted software, data, or other sensitive information.

Note Regarding E-mail
Technical data, including technical discussions about controlled technology projects, should not be transmitted, discussed or attached in email, whether international or domestic. If you have a mission-critical need to share information with your approved project team members, you should consult with UAF OIT about special arrangements.

Note Regarding Encryption
Encrypting your files, or the complete hard disk, is generally considered a best practice for data security. However, doing so when travelling internationally can create an additional set of issues. Some countries, including China and Russia, restrict the import of encrypted devices, and U.S. regulations prohibit the export of an encrypted device to any embargoed country.*

** Embargoed countries with restrictions on encryption currently include Cuba, Syria, Sudan, North Korea and Iran. Check with the Department of Treasury Office of Foreign Assets Control for the most up-to-date information; the embargoes and sanctions change frequently.*

See https://www.bis.doc.gov/index.php/policy-guidance/encryption for more information on encryption.