Guidance for Foreign Travel with Computers and Other Electronic Devices

Contacts:

Export Control Officer- Dr. Rani Muthukrishnan (rani.muthukrishnan@tamusa.edu)

Chief Information Security Officer- David Mendoza (dmendoza@tamusa.edu)

Empowered Official- Dr. Vijay Golla (Vijay.golla@tamusa.edu)

Reference:

System guidance regarding International Travel:

https://rso.tamus.edu/home/research-security/export-controls/intl-travel/#1600961463687-773af199-d43e

Guidance for San-Antonio campus:

When travelling abroad on official business, or you have to complete official business on vacation, all faculty and staff should get a loaner laptop from the ITS.

Here is the process to receive a loaner laptop for travel:

- Follow this link ITS Helpdesk Portal.
- Select I have a Jaguar account
- Block one: Request a loaner desktop/laptop
- Details: e.g. Customer will be instructing from a foreign country and will need VPN and Bitlocker
- Other users who will receive emails: iso@tamusa.edu

Export Controls Officer will also be notified.

Other Electronic Devices

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

- **Hardware.** Generally speaking, computer hardware is not subject to tight restrictions, as long as the hardware returns to the US. 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., www.microsoft.com/exporting/). The most significant restrictions pertain to encryption software. Commercially-available software (including the VPN software provided by TAMUSA) can be installed on devices that otherwise qualify for the exemptions listed below. Non-commercial encryption software in source code or object code is likely to be restricted; please check with the Export Control officer (210-784-1223) if you have questions.
- **Controlled data**. If you are working on a project that involves EAR or ITAR controlled technologies, your device may contain controlled technical data that cannot be shared with foreign parties without a license. **It is strongly recommended that you not take a device with such data outside the US**. If you do, it is critical that you inform the Export Control office if such data may have been compromised while traveling due to the device being lost, stolen, or outside your control.
- **Other private data**. Aside from export control laws, University policies regarding protection of student, financial, and HIPAA-controlled data recommend that such data not be stored on devices taken outside the US.

If the computer or other equipment is owned by the TAMUSA, the equipment as well as any pre-loaded 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 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 traveler) involves embargoed countries*.

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 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. (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. *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.* 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 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 is to be used only for making presentations, consider taking a memory stick or storing the presentation on a cloud-based server instead. If you are using a 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.

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 the TAMUSA Office of Information Security about the possibility of special arrangements.

General 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 Export Controls Officer (rani.muthukrishnan@tamusa.edu).

** 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.*

Adapted from the following sources:

1. University of California: https://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/laptop-slides.pdf
2. What to Know When Bringing Tech Devices through US Customs https://it.wisc.edu/news/know-bringing-tech-devices-us-customs/
3. Foreign Travel with Computers and other Electronic Devices https://www.colorado.edu/researchinnovation/ori-compliance/export-controls/guidance/international-travel