Dear Traveler,

Recently, there has been an increase in several hazards to international travelers. These include technology and identity theft. The theft of personal information may damage you personally and financially. Allowing sensitive information or research to be disclosed while abroad may violate U.S. Export Control laws. Violations can subject you as an individual, and the University as an institution, to possible criminal and civil penalties. The following tips will help minimize your risk. If you have any questions about these guidelines, please contact the Export Control Administrator at 491-1563 or scot.allen@colostate.edu. Additionally, please consider the following:

**Am I taking any physical equipment with me?**

Lab equipment, electronics, and other materials may require prior approval or documentation, depending on your destination. Please contact the Export Control Administrator for more info.

**Am I taking a laptop, smartphone, or other media device?**

While export control laws allow for travelers to take laptops for personal/teaching use to most locations, these must remain under your control at all times, and must return with you to the U.S. at the end of your trip. Do not leave your computer in your hotel room or other accommodations while on excursions or attending events, such as daytrips or dinners. If taking a smartphone or tablet, maintain control of the device at all times, turn it off when not needed, and ensure it is password protected.

Theft of information is also commonly performed when travelers utilize internet services, such as using Wifi internet networks or plugging into an Ethernet port. Your user IDs and passwords can be observed by key loggers, and your contacts and personal information may be downloaded without your knowledge. If you have a smartphone or tablet, it is recommended that you use your cell data plan for internet/email needs, and avoid local networks.

Do not update any software or allow other changes to your computer through foreign internet connections. The FBI has recently identified malicious software that may be disguised as an update to a legitimate program, like Adobe Flash Player.

**Am I taking any data, information, or research?**

CSU highly recommends that you take only the information you need, and if possible, send ahead or take only a flash-drive containing your presentation or relevant information. Do not take any information related to research that is export controlled, unpublished, or unrelated to the purpose of your visit. Likewise, remove personal information you would not want publicly disclosed. Some departments or colleges may be able to loan you a scrubbed laptop.

The fact that an academic traveler merely carries certain information or software to another country on a laptop or other storage device is sufficient for federal agencies to consider the information or software exported to that country, even if not actively used by the traveler in a presentation, discussion, or research while abroad.

*If you have any questions or concerns, please contact the Export Control Administrator at 491-1563, or scot.allen@colostate.edu, or consult [http://ricro.colostate.edu/Exportcontrol/ExportControl.htm](http://ricro.colostate.edu/Exportcontrol/ExportControl.htm).*