Best Practices to Maintain Security of Controlled Technology or Technical Data during International Travel

Introduction

Academic personnel including faculty investigators, graduate students or research fellows, and undergraduates travel internationally to attend or present at conferences and meetings, to collaborate with colleagues at other research institutions, and to perform field research. It is important to note that the academic traveler's failure to comply with U.S. export control laws can have grave consequences for the traveler and WVU. The traveler is ultimately responsible for compliance.

The Department of Commerce (Export Administration Regulations - EAR), the Department of State (International Traffic and Arms Control Regulations - ITAR), and the Department of Treasury (Office of Foreign Asset Controls - OFAC) have regulations that govern items which a traveler may take on international travel such as:

- Laptop computers, smart phones, tablets, etc.;
- Encryption products on your laptop computer;
- Data/Technology;
- Blueprints, drawings, schematics etc.

Academic personnel must consider the potential effect of each set of U.S. export control regulations on the proposed international travel to assure that both the institution and the individual traveler are in compliance. The Department of Commerce and the Department of State are principally concerned with whether the academic traveler will take and then disclose (intentionally or unintentionally) any controlled technology or other controlled information to non-U.S. persons (e.g. in papers, in personal conversations, on their laptop computers, or other electronic storage devices) or will export any controlled items (e.g., sensors, test instrumentation, reagents, biological materials or other similar tangible goods) to non-U.S. persons. The Department of Treasury is most concerned with the specific entities (institutions, companies, and persons) which the traveler may interact with or do business with while traveling abroad. . A U.S. person is defined as a U.S. citizen, a U.S. permanent resident, or a person having protected status in the U.S.

Traveling with Electronic Devices or Data

A U.S. person travelling abroad may take a WVU-owned laptop computer, smart phone, tablet, etc. to most countries without a license or license exemption or exclusion. While visiting some embargoed countries, a laptop computer, smart phone, tablet, etc. may be carried by a US person provided the laptop computer is kept under the traveler's effective control* and is **returned to the United States not more than one year** after the original departure date. It may be necessary to complete the TMP/BAG exclusion form prior to traveling to embargoed countries if the traveler is taking a laptop computer, smart phone, tablet, etc. The Export Control Office will inform the traveler if their trip requires a TMP/BAG exclusion based on information provided by the traveler.

**Effective control:* The traveler maintains effective control over an item when they either retain physical possession of the item, or secure the item whereby no other person may gain access to the item without engaging in criminal activity.

Vacation or Personal Travel

Travelers taking WVU-owned equipment on personal or vacation travel or accessing WVU e-mail while abroad must send a signed copy of this form to the Export Control Office (ECO) prior to departure if they haven't already done so in the fiscal year when the travel occurs and must notify the ECO of what WVU-owned equipment they are taking and their destination. If the traveler is not taking any WVU-owned equipment or accessing WVU e-mail while abroad, it is not necessary to contact the ECO regarding personal travel unless the destination is an embargoed country.

Any person traveling to an embargoed country for any reason needs to consult the ECO as soon as the trip is planned.

Guidelines to Remain Compliant

To ensure that the traveler does not run the risk of releasing sensitive information or technology when traveling abroad, or dealing with sanctioned countries, entities, or individuals, keep the following guidelines in mind:

- 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 travelling to non-embargoed countries:
  - Research which qualifies for the fundamental research exclusion
  - Openly published information
  - Publically available information
  - Unrestricted academic information
  - Publically available software
  - Issued patents and published patent applications

- DO NOT allow any person to connect a USB flash drive or other external storage device to your laptop computer or other electronic devices.

- DO NOT access WVU file servers or remote desktop computers.

- DO NOT access WVU e-mail or personal e-mail involving WVU related information from an unsecured network or WiFi connection. Do not transmit export controlled information even over a secured connection even if the information is encrypted. Encrypted information is still controlled by export control laws.

- When accessing WVU e-mail while abroad, use ONLY the web-based Office 365 client NOT the desktop client or a mobile application on a smart phone or tablet. The desktop client and mobile applications download all e-mail and attachments to the local device which makes accessing e-mail much more risky while traveling abroad. Use only a web-based client for accessing any e-mail when using your smart phone or tablet if there is any chance that you will be receiving export controlled e-mails while you are traveling abroad so that such e-mail and related attachments will not be downloaded to your local device.

- DO NOT open any e-mail attachments you suspect contain may export controlled information.

- Change your MyID password immediately upon return from international travel if you have used this password to access WVU e-mail or for any other purpose during your travel.

- If at all possible, take a clean, department laptop computer configured specifically for international travel rather than your work or personal laptop computer. A clean laptop computer is one which has been screened by OIT personnel to be clean of all malware, viruses, etc. and contains only standard the Microsoft Suite and Adobe Suite of software. The clean laptop computer is to be re-screened by OIT personnel upon your return before it is connected to any University systems including wireless or wired networks.

- The FBI warns that in some countries, the simple act of turning on your laptop computer while WiFi is enabled (or if you connect to wired network) will result in ALL files and information on your

computer being copied. Therefore, you should assume that everything stored on your computer or connected to your computer will be viewed by others when you are traveling abroad.

- Be aware that keyboard logger devices or malware may be recording your keystrokes on your electronic device while you are in airports, hotels, restaurants etc.
- Don't use telephones, computers, and fax equipment at foreign hotels or business centers for anything not currently in the public domain.
- If any electronic devices are stolen, file a police report and notify the ECO as well as OIT as soon as possible. Also notify the ECO and OIT immediately if any electronic devices are lost.
- Other precautions may be necessary depending on the traveler's destination. The ECO will notify the traveler of these prior to departure.

Preparing your electronic devices before leaving the U.S.:

- Remove anything from any electronic device that constitutes a trade secret, proprietary information, export-controlled technical data/information or anything you wish to keep confidential prior to leaving the United States.
- ***Deleting a file is NOT enough.*** Use a **"Shredder"** program to erase the information you do not want to share so that it cannot be recovered.
- Keep your work files on an encrypted flash drive or an encrypted external hard drive.
- Delete any saved passwords.
- Keep all electronic devices in your carry-on luggage.

Remember: If you don't need it - don't take it with you!!

I certify that I have read the above best practices information and understand it. I will contact the WVU Export Control Office (ECO) if any questions arise regarding best practices for protecting export controlled technology and information. I agree to comply with any additional instructions the ECO may need to convey to me in accordance with my specific travel plans. I understand that the traveler is responsible for export control compliance.

Traveler's Name:

Traveler's Hand Written Signature:

Date:

*This document must be read and signed by international travelers once per fiscal year as part of the Export Control Office review of international travel. Please send the ECO an electronic copy of the signed document. The ECO will maintain records of the signed documents and will request that a newly signed document be submitted for an international traveler if the latest signed document on file has expired.