**Important information for faculty and staff when traveling internationally**

Foreign travel with a laptop computer, PDA, cell phone, or data storage device
When you travel outside of the United States (except Canada), your laptop computer, PDA, cell phone, data storage devices and encrypted software may require an export license or other government approval to be taken to many countries outside of the United States. Most commercially available laptops and other devices that do not contain high encryption software (>64 bit key length) are eligible for an export exception TMP for “tools of the trade” when the following conditions are met.

1) complete the CMU Export Foreign Travel form annually to meet the recordkeeping requirements (pg 4)**\***

2) return the item(s) to the US within one year;

3) maintain “effective control” of item(s) during the duration of your trip;

4) do not take item(s) that contain high encryption software;

5) do not travel to or through an embargoed country (**Syria, Sudan, Iran, North Korea, or Cuba**)

***\*****The University is required to document the export (even a temporary export) of these items if they are owned by the University. The CMU Export Foreign Travel form only needs to be completed annually and updated if you add more foreign countries.*

“**Effective control**” is defined as actual physical possession or placed in a secure place like a hotel safe. Leaving your laptop in your hotel room or in an open conference room is not considered effective control.

US Customs officials are authorized to search or retain electronic devices, including digital cameras, cell phones, media players, and disk drives as well as the items listed above, even without probable cause, to look for violation of export control regulations as well as other laws and regulations. To prepare for this possibility:

1. Don’t carry data you don’t want others to see: medical records, data files from your research, financial information, photos, unpublished research, etc.

2. Don’t carry the only copy of data you can’t afford to lose.

3. Have a “Plan B” if there is data you will need when you reach your destination.

4. Consider taking a minimal device equipped with only ordinary, recognizable software and minimal data so any search can be fast and the consequence of a loss less disruptive.

## May I take my encrypted laptop when traveling internationally?

It depends. Sharing, shipping, transmission or transfer (exporting) of almost all encryption software in either **source code** or **object code** is subject to US export regulations. Most publicly available "dual-use" encryption code requires a license or License Exception to ship outside the U.S. In addition, US persons are prohibited, without prior authorization, from providing technical assistance (i.e., providing instruction, skills training, a working knowledge, and consulting services) to a foreign national with the intent to assist in the overseas development or manufacture of encryption software that is subject to U.S. Government notification or authorization.

## What U.S. export controls do I need to satisfy when leaving the country with my encrypted laptop?

You will need to determine which encryption software will be on your laptop or other electronic device to determine if an ENC license exception is available. For example, encryption software like Symantec Encryption products or McAfee's Data Protection Suite, qualify for ENC license exception (EAR 740.17).  This exception allows university employees to hand-carry, transport or ship a University-owned or personally-owned computer that has Symantec or McAfee's encryption products installed to any country except embargoed countries as long as the computer remains under your “effective control”.

## Which countries are subject to United States embargoes and require a license?

***Cuba****,* ***Iran****,* ***North Korea****,* ***Sudan****,* ***Syria***

If you must travel to one of the five embargoed countries listed above, contact CMU’s Export Compliance Officer for guidance on applying for a license. The license process can take, at least ninety days.  The [Department of Commerce’s Bureau of Industry and Security](http://www.bis.doc.gov/) and the [Office of Foreign Assets Control (OFAC)](http://www.treas.gov/offices/enforcement/ofac/) within Dept. of Treasury accept applications for licenses for travel to embargoed countries. Note that each embargoed country application is evaluated on a case-by-case basis, subject to different sanctions, and a license may be denied. You may not travel to these countries without a license from the U.S. Government.

Are there other high risk countries that require export review by CMU’s Export Compliance Officer (ECO)?

 Yes, regardless of your research or activity you should contact the ECO if you are traveling to the following countries for specific guidance and a travel briefing. *Afghanistan, Balkans, Belarus, Burma, China, Cote d’Ivoire, Democratic Republic of Congo, Eritrea, Haiti, Iraq, Lebanon, Liberia, Libya, Sierra Leone, Somalia, Venezuela, Vietnam, and Zimbabwe.*

## Which foreign countries have encryption import and use restrictions and how can I obtain an import permit?

Since laws can change at any time, please check with the [US State Department](http://www.state.gov/misc/list/index.htm) before travelling internationally to ensure that you have the most up-to-date information.

CMU can only provide basic guidance in this area. The most current (Jul 2010) resources found, list the following nations that may not recognize a "personal use exemption".  Before traveling to these countries with an encrypted laptop, you may want to check with the specified governmental agency if a permit is required for an academic institution laptop.

* **Belarus** - a license issued by the Belarus Ministry of Foreign Affairs or the State Center for Information Security of the Security Council may be required.
* **Burma (Myanmar)** - a license may be required, but licensing regime documentation is unavailable. Contact the [US State Department](http://www.state.gov/aboutstate/) for further information.
* **China** - a permit issued by the Beijing Office of State Encryption Administrative Bureau may be required. You can either apply for the permit on your own, or contact our McAfee authorized distributor.
* **Hungary** - an International Import Certificate is required. Contact the [US State Department](http://www.state.gov/aboutstate/) for further information.
* **Iran** - a license issued by Iran's Supreme Council for Cultural Revolution is required.
* **Israel** - a license from the Director-General of the Ministry of Defense may be required.  For information regarding applicable laws, policies and forms, please visit the following website: <http://www.mod.gov.il/pages/encryption/preface.asp>.
* **Kazakhstan** - a license issued by Kazakhstan's Licensing Commission of the Committee of National Security may be required.
* **Moldova** - a license issued by Moldova's Ministry of National Security may be required
* **Morocco** - a license may be required, but licensing regime documentation is unavailable. Contact the [US State Department](http://www.state.gov/aboutstate/) for further information.
* **\*Russia** - licenses issued by both the Federal Security Service (Federal'naya Sluzhba Bezopasnosti - "FSB") and the Ministry of Economic Development and Trade may be required. License applications should be submitted by an entity officially registered in Russia. This would normally be the company that is seeking to bring an encryption product into Russia.
* **Saudi Arabia** - it has been reported that the use of encryption is generally banned, but research has provided inconsistent information.  Contact the [US State Department](http://www.state.gov/aboutstate/) for further information.
* **Tunisia** - a license isued by Tunisia's National Agency for Electronic Certification (ANCE) may be required.
* **\*Ukraine** - a license issued by the Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine (SBU) may be required.

## What can I do if I cannot satisfy encryption export or import control requirements?

CMU faculty or staff can request a "clean laptop" from your department, if available.  A clean laptop is a computer that is preloaded with standard University software, but does not contain high encryption software or sensitive data that could put you or the University at risk if the laptop is lost or stolen.

PLEASE COMPLETE THE FORM ON THE NEXT PAGE TO USE THE TOOLS OF THE TRADE EXEMPTION AND SEND A COPY TO STREXLER@ANDREW.CMU.EDU

**PLEASE CARRY THE SIGNED ORIGINAL WITH YOUR TRAVEL DOCUMENTS.**

**YOU MAY NEED THIS DOCUMENT FOR CUSTOMS WHEN YOU ENTER OR EXIT ANY COUNTRY INCLUDING THE UNITED STATES.**

**TMP EXEMPTION - Terms and conditions of exporting CMU items, technology or software**

1. I will take the item(s) and/or software abroad **ONLY** as a "tool of trade" to conduct Carnegie Mellon business; and

2. I will return the item(s) and/or software to the US no later than 12 months from the date of export unless they are certified by me to have been consumed or destroyed while abroad during this 12 month period; and

3. I will maintain the item or software under my "effective control" while abroad ("effective control" means retaining physical possession of an item or maintaining it in a secure environment such as a hotel safe or a locked or guarded facility; and

4. I will not take items, technology, technical data or software to Cuba, Iran, North Korea, Syria, or Sudan; and

5. I will not take outside the borders of the United States any items or software incorporating non-commercial encryption source code:

\* Employing a symmetric algorithm with a key length in excess of 64 bits;

\* Designed or modified to perform dual-use cryptanalytic functions;

\* Designed or modified to use quantum cryptography;

\* Using cryptography in communications cable systems designed or modified to detect surreptitious intrusion using mechanical, electrical or electronic means;

\* Using cryptographic techniques to generate channelizing codes, scrambling codes or network identification codes for systems using ultra-wideband modulations techniques; and

6. I will review export controls with the ECO before taking/sending any Carnegie Mellon equipment, new or proprietary technology, unpublished technical data, or CMU created software abroad; and

7\*. While outside the U.S., I will promptly report all instances where unauthorized access is suspected; and

8\*. I will promptly report, the loss or theft of any item, encrypted software, or technical/sensitive information to Carnegie Mellon; and

9. I understand that I may be held personally liable for violations of U.S. export laws that are punishable by severe civil and criminal penalties, including monetary fines and imprisonment.

Countries traveling to

Description of CMU item(s), technical data, or software to be taken abroad:

Traveler Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:

Printed Name:      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:       Dept:

Update as needed:       Date:

**PLEASE CARRY THE SIGNED ORIGINAL WITH YOUR TRAVEL DOCUMENTS. YOU MAY NEED THIS DOCUMENT FOR CUSTOMS WHEN YOU ENTER OR EXIT ANY COUNTRY INCLUDING THE UNITED STATES. Contact Sheryl Trexler, ECO if you have any difficulties while traveling abroad 412-268-2841.**