INTERNATIONAL TRAVEL AND EXPORT CONTROL REGULATIONS

When planning a trip abroad, individuals sometimes take information, technology and equipment with them. However, faculty, staff and students need to be aware of the impact of export control regulations when traveling internationally. Export control regulations affect:

- Items you take with you on a trip:
  - Laptops, smart phones (both personal and Rensselaer-owned),
  - Encryption items,
  - Data and technology,
  - Blueprints, drawings, and schematics, and/or
  - Chemicals, biological materials, and scientific equipment.
- Supplying certain technologies or data at a “closed” conference or meeting (a meeting that is not open to all technically qualified members of the public and attendees are not permitted to take notes).
- Restricted information (in print and electronic format or discussed verbally while abroad).
- Travel to sanctioned or embargoed countries.
- Conducting business with, or providing services to, certain people or entities (including human subjects and collaborative research).
- You must maintain Effective Control of electronic devices.

You must ensure that any information you discuss or items you take are either not controlled or if controlled, the proper export control licenses are in place. A license may be required from the Departments of Commerce, State, and/or Treasury depending on the items you are taking, the country you are traveling to, and the individuals you will be interacting with.

Fortunately, travel to most countries oftentimes does not raise any export control concerns. In some cases, an exclusion or exception to the license requirements is available. In order to assess any export control restrictions associated with your upcoming international trip, please answer the following questions carefully. Note: Individuals can be held personally liable for exporting items, technical data, or software without a license or license exception.

Travel Clean: If it is possible, it is recommended to travel internationally with a clean laptop so that it can be completely wiped clean prior to and upon return.

Effective Control: Export Control Regulations require you maintain effective control over an item when you either retain physical possession of the item, or secure the item in such an environment as a hotel safe (not hotel room safe), a bonded warehouse, or a locked or guarded exhibition facility. Leaving a laptop unattended in your room while away is not Effective Control and not in compliance with U.S. Export Control laws and regulations.

If you have any questions, please contact Rensselaer’s Export Control Office (518-276-3777) or email: exportcontrol@rpi.edu.
1. Do you plan to travel to an embargoed destination?
   Note: Certain countries such as Burma, Cuba, Iran, Ivory Coast, Libya, Liberia, North Korea, Sudan, Syria, and Zimbabwe face increased restrictions. For a list of OFAC embargoed countries and other restrictions, please visit: www.trens.gov/offices/enforcement/ofac/programs.
   □ Yes □ No

2. Will you be taking any information or technology that is not widely available in the public domain, is classified, or is subject to export control regulations?
   (Including materials in print or electronic versions)
   **Export controlled** materials include technology, software, and information related to the design, production, testing, maintenance, operation, modification, or use or controlled items or items with military applications. It does not include basic marketing information on function or purpose; information regarding general scientific, mathematical or engineering principles commonly taught in universities; or information that is generally accessible in the public domain.
   □ Yes □ No

3. Are you taking any biological or hazardous materials abroad?
   If yes, have you obtained approval and appropriate licenses?
   □ Yes □ No □ Yes □ No

4. Will you be taking any materials or equipment with you? (Including a laptop computer, software, scientific equipment, etc)
   □ Yes □ No

5. Will you be attending a "closed" conference or meeting?
   Note: A closed meeting is not open to all technically qualified members of the public.
   □ Yes □ No

6. If you will be presenting at a conference or meeting, will you be presenting information that is *not* available in the public domain or fundamental research?
   □ Yes □ No

7. Will you be providing a service or financial assistance to a foreign entity or person while traveling internationally?
   Note: "Financial assistance" includes hiring of project personnel. "Services" include providing medical assistance, assisting in data analysis, discussing technical designs, etc.
   □ Yes □ No

8. Will you receive compensation for your travel expenses or other compensation from a foreign sponsor or government?
   □ Yes □ No

9. Will you be sharing Rensselaer developed, non-commercial encryption software in source code or object code?
   □ Yes □ No

10. Do you know or have any reason to believe that the information you will be sharing or the activities you will engage in while traveling will have a military use or will provide a military service?
    For example, will the information you carry with you or the discussions you have, aid in the design, development, production, stockpiling or use of nuclear explosive devices, chemical or biological weapons, or missiles?
    □ Yes □ No

It is to be understood that an international traveler could be personally liable if they unlawfully export or disclose export controlled information or technology to foreign nationals without prior approval.
Best Practices
For
Academics Traveling Overseas

American academic freedom and the advanced research & development (R&D) conducted at Academic Institutions have resulted in progress in innumerable areas. But, there are still some considerations to help protect your students and your R&D from being stolen by other researchers, or used by hostile foreign governments / their military agencies:

Prior to your travel, be sure to visit http://travel.state.gov/travel/travel_1744.html or https://www.cia.gov/library/publications/the-world-factbook/index.html to obtain country background, updated travel advisories and the current political situation of the countries being visited.

Do not travel with any unnecessary information or current research on a laptop. Avoid placing internet addresses ("favorites") on any laptop you take. Take only that info which you will present or discuss at the conference. Do not leave your laptop unattended. Make sure your laptop is password protected. Do not continue to use a laptop that begins to run slowly, or acts strangely after taking it overseas. Have the system professionally analyzed for viruses or spyware before and after travel. Recognize that your personal belongings may be searched several times.

Understand that foreign universities, foreign companies, and foreign governments are often interconnected, such that any inquiry (personal or electronically) while traveling, actually may be from a hidden interest with an ulterior motive.

Not all conference attendees with whom you come in contact with are genuinely interested in your research. Some may be inquiring on behalf of another country or researcher.

Be aware of unsolicited requests sent to you on the internet, persons asking questions about your research, and persons requesting your opinion as to the status of others’ research being conducted at the Academic Institution. Information about failures in research can be as valuable as successes. Be careful in discussing any research that is not your own.

Recognize not all foreign students who contact American professors are doing so on their own accord. Some are directed to do so by a competitor or a foreign intelligence services.

Obtain business cards of all personnel with whom you have extensive contact while traveling. Put the date of contact on the back and retain them for future reference.

Do not speak about, or comment on, the status of research and development being conducted by others in your department. Defer questions to those professors directly.

Avoid political conversations, or offering political opinions, while in foreign countries. This includes in person, on the telephone, or on the internet.

Do not take any provocative or suggestive literature with you to other countries.

After meeting with the appropriate representative from your Academic Institution, report any unusual personal, telephonic, or internet contacts to your local office of the FBI.
Counterintelligence Threat to Academic and Scientific Travelers

When you travel overseas in an academic or scientific capacity you are subject to intelligence collection by foreign intelligence and security services (FISS). FISS are responsible for identifying individuals who can give them access to people and information in the US as well as acquiring information that will advance indigenous research and development. Traveling academic and scientific delegations afford FISS an ideal opportunity to gather information on US subject matter experts.

- You are known to government institutions before travel because of your visa
- FISS are in a permissive environment when operating in their home country and can scrutinize you either by design or chance using one of many justifications:
  - Fitting a criminal, or other profile
  - Participating in “black-market” activity
  - Possessing a banned or strictly controlled material
  - Associating with persons whom the government views as dissidents
  - Having language fluency, declared relatives, or organizational affiliations in the country you are visiting

FISS intelligence collection operations are usually unobtrusive, non-threatening and conducted without your knowledge. Although less common, some FISS use more aggressive or provocative measures meant to intimidate or “test” your reaction. Intelligence collection methods used by FISS include:

- **Elicitation** – a ploy whereby FISS use seemingly normal conversation to extract information about your work and associates
  - Elicitation is the most noticeable form of intelligence collection
  - It can be difficult to identify and is easy to deny

<table>
<thead>
<tr>
<th>Examples of Elicitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct questioning</td>
</tr>
<tr>
<td>Normal curiosity</td>
</tr>
<tr>
<td>False statements</td>
</tr>
</tbody>
</table>

UNCLASSIFIED
UNCLASSIFIED

• **Exhaustion**—scheduling a lengthy or extensive itinerary of events and activities designed to tire visitors and make them pliable.
  o Drivers or guides frequently accompany visitors and engage in elicitation
• **Eavesdropping**—listening in on conversations for information
  o Usually in social settings (bars, restaurants, or public transportation, etc.) where talking “shop” often occurs
• **Technical Eavesdropping**—use of audio/visual devices (often concealed) installed in public and private facilities, especially hotels and restaurants
• **Surreptitious Entry**—entry into your hotel room (often hotel assisted), accommodation or office to access documents or electronic information
• **Electronic Interception**—Fax, Telex, cell phones, and the internet are vulnerable to monitoring due to government control of telecom infrastructure
• **Physical Surveillance**—monitoring of your movements and activities

Common sense and basic CI awareness can effectively protect you against FISS attempts to collect sensitive information. Things you can do include:

• Do not leave sensitive materials in hotel rooms or safes
• Do not use computers or faxes at hotels or business centers for sensitive material
• Do not discuss information with someone who does not have a reason to know it
• Keep your personal computer as carry-on baggage
• Do not leave cell phones or portable electronics unattended
• Do not attempt to locate listening devices
• Do not attempt to evade physical surveillance
• Report CI incidents when you return

In addition, there are several things you can do to successfully counter elicitation:

• Prepare talking points ahead of time that do not disclose sensitive information
• Do not engage in conversation alone
• Redirect the conversation
• Excuse yourself from the conversation
• Reply to a question with a question
• Provide vague or hypothetical responses
• Provide historical, publicly known information
• Change the topic
• Feign ignorance
• Ask “Why?”

If you observe any activity that seems to be out of character with the purpose of a foreign visit, please contact the FBI San Diego Field Office at 858-565-1255

UNCLASSIFIED