CUNY EXPORT CONTROL GUIDANCE: INTERNATIONAL TRAVEL BRIEFING

1. Introduction
When traveling abroad, taking certain items, providing certain services or meeting with certain people can present export control problems for CUNY faculty, staff, students and postdoctoral scholars (“CUNY affiliates”). This document provides guidance on how to avoid running afoul of the export control laws when travelling internationally. Travel to most countries does not present an export control problem. Travel to some countries may present a problem that is easily addressed, provided we create and maintain records that show we found the travel to be exempt from the regulations. But when an export control license is required for travel, it is crucial that we obtain it prior to the trip. Violations of the export control laws carry severe civil and criminal penalties. Toward the end of this document, we have provided helpful tips to keep in mind when travelling abroad.

2. Applicable Regulations
When traveling internationally, CUNY affiliates need to be familiar with export control regulations and policies. See http://www.cuny.edu/research/compliance/Export-Control.html. Specifically, they need to determine whether the following regulations apply to them:

- **US Department of Commerce’s Export Administration Regulations (EAR)**
  These regulations govern hardware, materials, equipment, software, technology and technical data that have both civilian and inherent military or defense application. Controlled items are identified on the Commerce Control List (CCL). EAR controls are specific based on the combination of 1) destination; 2) end use; and 3) item specifications and capability.

- **US Department of State’s International Traffic in Arms Regulations (ITAR)**
  These regulations govern 1) defense articles, to include hardware, materials, equipment, software, technology and technical data specifically designed or modified for defense or military application without civil performance or use equivalent; and 2) defense activities, to include disclosing ITAR technical data (or data related to a defense article) to foreign nationals, or disclosing technical data (even if not controlled or in public domain) to a foreign national or related organization affiliated with a military purpose.

- **US Department of Treasury’s Office of Foreign Assets Controls (OFAC)**
  These regulations restrict transactions with a specified list of embargoed countries and with certain “specifically designated nationals”. For the purposes of CUNY affiliates, restrictions that are most likely to affect CUNY exports are on Cuba, Iran, Syria and Sudan.

3. Evaluating Whether the Regulations Apply to You
In evaluating whether any of the regulations apply to your travel, you need to consider:

- Whether you plan to take any controlled items or data with you; the most common items that present export control issues are laptops, jump drives, hand-held GPS
devices, blueprints or schematics, encryption products and prototypes or samples that happen to be portable;

- Whether you plan to send or deliver any controlled items or data to non-US persons;
- Whether your laptop or other storage device you are taking has controlled data or information stored on it;
- Whether the country to which you are traveling has any OFAC restrictions;
- Whether you will be doing business (including engaging in money transactions or the exchange of goods or services) with certain people or entities that are considered “specially designated nationals.”
- Whether you will be supplying certain technologies/data at a "closed" conference or meeting (not open to all technically qualified members of the public, and attendees are not permitted to take notes)

4. Necessary Actions
If you believe any of the regulations might apply to you, you should contact the export control administrator for your College to determine whether any license exemptions apply to you; or to obtain appropriate license or authorization.

5. Helpful Tips - When traveling internationally:

- Use your best judgment in communicating with foreign nationals, and be alert to situations that may result in inadvertent, inappropriate or illegal disclosure of controlled information or data;
- Avoid situations that lead to providing advice or assistance outside of fundamental research parameters;
- Do not discuss controlled or sensitive information (for example, proprietary information that you may happen to have) in public places;
- Always keep controlled or sensitive items, information or data secure;
- Maintain a “need-to-know” policy when discussing work related information with others;
- Do not leave equipment, documents or data in your hotel safe;
- Ensure that CUNY has a way of getting in touch with you if necessary;
- Do not use non-CUNY issued computers to log into CUNY’s network;
• Do not allow foreign electronic storage media to access your phone or computer;

• Report stolen laptops, computers or other devices to US Embassy or Consulate; and

• Upon return:= meet with your IT Security Officer to review your system access; change all passwords, including the one for your voicemail; and report unusual incidents or tasking for information to your Export Control Administrator.

• NOTE: Travelers must be aware that the privacy and security they expect at the same name hotels in the US is NOT what they may encounter in emerging countries. US hotel corporations are often simply property managers operating under strict foreign law and oversight, with little ability to provide western-style hotel privacy and security. US hotel corporations must comply with foreign security officials having access to their hotels with no requirement to notify management. This includes access to guest lists, credit card information and to rooms.