EXPORT CONTROLS: (701) 231-6455 / ndsu.exportcontrols@ndsu.edu
OFFICE OF THE VICE PRESIDENT FOR RESEARCH AND CREATIVE ACTIVITY

NDSU's Export Control Office: International Travel Briefing

Traveling Outside the U.S.? You are about to Become an "Exporter"

- Any tangible items that you are taking to a foreign country are considered "exports" by the United States Government, even if you are planning on bringing the items back upon your return.

- Technical information located on your laptop's hard drive or in a hard copy notebook is considered to be an export of "technology"/ "technical data", once the laptop or notebook leaves the U.S.

- Even technical know-how that is in your head, if shared with a foreign national, is considered to be a type of export.

When you leave the United States, you need to know your responsibilities under export control regulations. In particular if you are traveling with your laptop or any other electronic devices these items along with the underlying technology, any data on your device, proprietary information, confidential records, and encryption software are all subject to export control regulations. Some foreign governments have regulations that permit the seizure of travelers' computers and the review of their contents. U.S. Customs officials are also authorized to review the contents of travelers' laptops without probable cause and can be held until your return.

Export controls issues can arise in a variety of surprising circumstances; are not always intuitive; and the laws are fact-specific, complex, and continually changing. Given this complexity, the NDSU community should seek guidance from NDSU's Export Control Officer (ECO) when dealing with export control questions and concerns:

Lynn Titus Jr., Export Control Administrator: (701) 231-6455 / ndsu.exportcontrols@ndsu.edu / NDSU's Research 1 Building. See also http://www.ndsu.edu/research/export_controls/miscellaneous/international_travel.html. to be directed to an appropriate authority regarding your questions, concerns, or to make reports of unscrupulous activities abroad or in the United States or its territories.

BRIEFING

The FBI considers the following to be threats to our national security, regardless of the country involved:

Any foreign intelligence activity that is:

- targeting U.S. intelligence and foreign affairs information and U.S. Government Officials or official representatives
- directed at critical technology
- directed at the collection of U.S. industrial proprietary economic information
- directed at the collection of information relating to defense establishments and national preparedness
- involving the proliferation of special weapons of mass destruction
- involving perception management and active measures

If you become aware of or suspect any foreign intelligence activity aimed at the above list, notify your local in-country FBI office.

Current Version: 04/19/17.

PRIOR TO DEPARTURE

1. You may also want to contact the Department of State recorded messages at 202-647-5225.

2. Carefully complete your Visa application, as it will be scrutinized. If you are a naturalized U.S. citizen returning to the country of your origin, your citizenship may be questioned.

3. Ensure that items you carry with you are not controversial or prohibited. Political material or anything that could be considered pornographic should not be carried. If you carry prescription drugs with you, be certain that they are clearly marked and bring only necessary quantities.

4. Carrying letters, packages or gifts to individuals in other countries should be avoided. You may be viewed as a courier attempting to bring the material for subversive or illegal purposes.

5. DO NOT TAKE CONTROLLED MATERIAL with you as you travel.

6. Limit the amount of identification that you take. If you have several forms of Government ID (i.e. University ID, building pass), bring only one ID with you (or the minimum required for entry and exit). Make a photocopy of any ID or credit card you will be bringing and leave the copy at home. Write down your passport number and keep it separate from your passport. Do the same with your address and telephone.

7. The carrying of laptop computers is discouraged, but not prohibited. Consult your sponsor's contracting officer before you take your laptop or similar computing equipment.

UPON ARRIVAL

1. (If required) an accurate declaration of all money and valuables should be made at entry. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money exchanges, these frequently are required upon departure. Undeclared sums of U.S. or other currency are likely to cause difficulty with authorities and may be confiscated upon departure.

2. (If required) Declare such items as cameras, radios, etc., to preclude possible explanations, customs charges, or confiscation when you leave.

3. In some cases, especially non-westernized countries like Cuba, Syria, N. Korea, etc. you should contact the American Embassy or Consulate prior to your arrival, and provide your local address and the probable length of your visit.

4. Use of public transportation is recommended rather than driving yourself, because involvement in traffic accidents can be problematic. Taxis are the preferred mode of transportation. State Department travel advisories provide updated information regarding public transportation concerns in the country you are visiting.

YOUR ACTIVITIES AND BEHAVIOR

1. In all of your activities, show discretion and common sense. MAINTAIN A LOW PROFILE. Refrain from any behavior that may make you conspicuous or a potential target. NEVER engage in any illegal activity, excessive drinking or gambling. Use your best judgment to carefully avoid any situation that may allow a foreign intelligence agency the opportunity to coerce or blackmail you.

2. Do not discuss controlled or sensitive information in any vehicle, restaurant, hotel room, hotel lobby, or other public place. In any public place, your conversation may be overheard, or you may be monitored. If you need to call the U.S.

to discuss controlled or sensitive information, locate a secure telephone by contacting the in-country FBI office or the U.S. Embassy.

3. If you locate any possible surveillance equipment, such as microphones, telephone taps, miniature recording devices, or cameras, do not try to neutralize or dismantle it. Assume the device is operable and that active monitoring is ongoing. Report what you have found to the U.S. Embassy or Consulate. When you return, advise your local FBI agent.

4. Never leave luggage or briefcases that contain controlled or sensitive information unattended (whether in the US or US Territory or not). This includes leaving your briefcase in your hotel room. We encourage you to keep your briefcase containing sensitive information in your immediate possession at all times.

5. Foreign Intelligence Services may place you under physical surveillance or you may suspect that you are being watched. It is better to ignore the surveillance than attempt to lose or evade it. In any event your actions should be prudent and not likely to generate suspicion. Good precautionary measures are to use well-traveled highways and avoid establishing routine schedules.

6. Never try to photograph military personnel, installations, or other "restricted areas". It is best to also refrain from photographing police installations, industrial structures, transportation facilities and boarder areas.

7. Beware of overly friendly or solicitous people that you meet. Do not establish personal or intimate relationships with these individuals as they may be employed by the intelligence service. Do not share any work related information with any person who does not have a need to know.

8. Do not accept packages and agree to transport them back to the U.S. Even if your friends, relatives, and professional contacts, make the request, do not accept the package.

9. If you will be on an extended visit and expect to be writing or receiving mail, remember that it may be subjected to censorship. Never make references to any controlled or sensitive information.

10. Avoid any areas where there is political or ethnic unrest, demonstrations or protests.

11. Should you be detained or arrested for any reason by the police or other officials, be cooperative, and contact the U.S. Embassy or Consulate immediately. Do not make any statements or sign any documents you do not fully understand until you have conferred with an Embassy representative.

12 .Do not leave documents in hotel safes.

13. You may keep this travel briefing document for reference, but do not carry it with you.

UPON YOUR RETURN

Contact your local FBI agent to report suspicious foreign contacts and any unusual incidents. If you have a security clearance through a third party, you may need to receive a security debriefing if you have been abroad for more than a certain number of days that is established by the third-party security office. You are required to report all contacts with individuals of any nationality, either within or outside the scope of your official activities in which:

- Illegal or unauthorized access is sought to controlled or sensitive information.
- You are concerned that you may be the target of an actual or attempted exploitation by a foreign entity.

Note: This document was adapted from several "Defensive Security Briefings" found at national laboratories around the USA.

Plan Ahead to Avoid Violations – Work With Your Export Control Office

Just because an item is listed on the CCL does not mean that you cannot take it with you to your destination country. Export restrictions on CCL items vary, depending upon your destination country, those to whom you expect to release such items, and how you expect they will use them. Even if a license is indicated for your export, it is usually possible to find a documented reason why technical information can be excluded from regulation or a license exception for exported tangible items. Similar forgiveness can often be found in regulations that other agencies apply to your travels, such as the sanction programs.

Working with your Export Control Office well ahead of your international journey is the best way to ensure that your exported goods and information can be taken / sent without a license or violation of the export control and sanction program regulations. If any Risk Factor above is present in your planned travel, please contact:

Lynn Titus Jr., Export Control Officer
(701) 231-6455 / ndsu.exportcontrols@ndsu.edu / NDSU's Research 1 Building.
***See also* http://www.ndsu.edu/research/export_controls/miscellaneous/international_travel.html.**

http://travel.state.gov/content/passports/english/alertswarnings.html

Three Noteworthy Federal Agencies that Have Jurisdiction over You and Your Exports:

- The Department of State's Directorate of Defense Trade Controls (DDTC), which implements and enforces strict controls upon tangible items and technical data that are determined to have been "specifically designed, developed, configured, adapted or modified for a military application." Such items and data can be found listed on the U.S. Munitions List in the DDTC's International Traffic in Arms Regulations.

- The Department of Commerce's Bureau of Industry and Security (BIS), which implements and enforces regulations that prohibit the release of certain commodities and information to certain countries or to their citizens (regardless of their location), if it is believed that there is a potential for such items to be used to undermine U.S. security, policy, or other vital interests. Such items are often referred to as "dual-use" items and can be found on the Commerce Control List (CCL) in BIS's Export Administration Regulations (EAR). Note that many items on the CCL are commercially available in the U.S.

- The Department of the Treasury's Office of Foreign Assets Control (OFAC), which prohibits varying types of transactions (e.g., financial, commercial, and even academic) and activities with or in foreign countries (or with their citizens, regardless of location) through its sanction programs, which are designed to encourage other countries', entities', or individuals' cooperation with U.S. policies and interests worldwide.

I'm Just a University Employee. Why Should I Have to Worry About These Agencies' Regulations?

- Depending upon their areas of expertise, NDSU employees may work with items and foreign countries covered by DDTC, BIS, and OFAC regulations.

- US Customs officials are authorized to search or retain electronic devices and other items leaving the U.S., even without probable cause, to look for violation of export control and sanction program regulations.

- Other universities and/or their employees have, by violating export control or sanction program regulations, exposed themselves to steep financial penalties and incarceration.

Risk Factors Contributing to Violations

If any of these factors apply to your planned travel, please contact the NDSU Export Controls Office before you travel by using the contact information provided below.

- **Sanctioned Countries**
  - Will you be traveling to a country subject to OFAC sanctions?
  - Each sanction program is different from the other. Some programs broadly prohibit imports and exports of goods, technology and services from / to certain countries. Other programs only prohibit transactions with certain listed entities and individuals. Sanction programs change over time, sometimes rapidly, as world events affect the U.S. Government's relationship with other countries and governments.
  - Before you travel, visit the OFAC website to determine whether you will be visiting a sanctioned country.
- **Restricted People and Entities**
  - Do you expect to enter into transactions with persons or entities that the federal government has determined must be excluded from such transactions?
  - We recommend that you search a Consolidated Screening List for the foreign parties with whom you expect to interact professionally during your international travel.
- **Defense Articles and Data**
  - Will you be taking to any foreign country tangible items or information related to research or other activities that support defense-related projects or objectives? One should note that the DDTC presently considers not only things like missiles and fighter jets to be defense articles, but also spacecraft designed for scientific objectives. This includes scientific satellites and other space-related equipment, including support apparatus, such as launch platforms and telemetry stations.
- **Commerce Control List Commodities and Technical Information**
  - Will you be taking with you commodities or technical information found on the CCL?
  - The only way to know for certain is to perform a keyword search on Title 15, Part 774 (a/k/a the "Commerce Control List"), which can be found in a searchable format at the GPO Access website. If provided sufficient notice before your international trip, your Export Control Office can assist with such a search.

- Risk of finding your items restricted for export by the CCL increases when:
  - Your travel will take you to one or more of the "T5" Countries, which consist of Cuba, Iran, North Korea, Syria and Sudan. Some or all of these countries are subject to not only heightened BIS export restrictions, but also to heightened export and transaction restrictions imposed by OFAC and DDTC.
  - You will be taking items related to your work at NDSU, including: a) tangible items, such as samples, prototypes, and equipment; and/or b) unpublished research technical data; AND you work in the following areas:

- ☐ Chemical, Biotechnology and Biomedical Engineering
- ☐ Materials Technology
- ☐ Remote Sensing, Imaging and Reconnaissance
- ☐ Navigation, Avionics and Flight Control
- ☐ Robotics
- ☐ Propulsion System and Unmanned Air Vehicle Subsystems
- ☐ Telecommunications/Networking Nuclear Technology
- ☐ Sensors and Sensor Technology
- ☐ Advanced Computer/Microelectronic Technology
- ☐ Information Security/Encryption
- ☐ Laser and Directed Energy Systems
- ☐ Rocket Systems
- ☐ Marine Technology

- Risk of finding your items restricted for export by the CCL decreases when:

    - You will be traveling to countries sharing a relatively friendly, cooperative relationship with the U.S., such as with the countries that belong to N.A.T.O. and other treaty-based groups.

    - Your work is in a field that is not fundamentally "technical", such as a discipline traditionally included in the humanities. However, beware of electronic and medical equipment exported in support of your overseas work, and don't forget that OFAC sanction regulations may still apply to your destination and your activities there.

    - The tangible items that you are taking are: (a) personal effects that most people need and use when they travel outside the U.S., and/or (b) such items will be under your effective control throughout your travel and will return to the U.S. with you within one year or less.

    - The work-related information that you take with you (e.g., on your laptop or other media)

        A. is already published and generally accessible to the interested public
        B. is available to anyone wishing to take a university catalog course
        C. was generated by basic or applied science and engineering and is the type of information that is ordinarily published and shared broadly within the scientific community (often referred to as the results of "fundamental research").

- A Common Question: What about my laptop, smart phone, or data storage device?

    - Short answer: It depends upon a device's features, the software or data that you have loaded on it, who owns it, the purposes for which you are taking it, and where you want to take it.

    - Fortunately, many of these items are listed on the CCL under Export Control Classification Number (ECCN) 5A992 and can be taken to most countries, except for those subject to embargoes and other heightened export controls.

    - The software that operates or is used on these items, including mass-market and open-source products, also can be found on the CCL (ECCN 5D992) and are controlled separately from the hardware on which they're used. If possible, we recommend traveling internationally with personally-owned laptops containing only software, technical data, and personal information considered essential for the trip.

- Newer, more advanced computing and communication devices (as well as associated software), especially those that provide exceptionally strong levels of encryption, may be difficult to take to other countries, especially the T5 countries. If you know or suspect that your electronic devices are more advanced than the average, it would be a good idea to determine what the items' ECCNs are by asking the manufacturer and working with your Export Control Office.

- Even though the CCL may indicate that a license is required to export your laptop to a particular country, a license exception can often be found that will allow you to export it on a temporary basis. For example:

    - Depending upon the country, you may be allowed to travel with a NDSU-owned laptop under a temporary export (TMP) license exception, if the laptop and your use of it qualify under BIS's definition of a "tool of the trade."

    - In other instances, you may only be able to take a laptop to another country if it qualifies for a baggage (BAG) license exception which, among other things, requires that the laptop be owned by the traveler.

    - When taking equipment and other export-controlled items to other countries under a license exception, you should understand the conditions under which the exception can be used. It is also a good idea to take with you a letter from your Export Control Office indicating that the license exception is being invoked for your temporary export.

Taking Electronic Devices

Researchers commonly travel with commercially available electronic devices such as laptops, PDAs, iPads, cell phones, drives, and other digital storage devices. These items often come with pre-loaded encryption software which is subject to the Department of Commerce, Export Control Regulations (EAR). Many of these items can be temporarily exported under the EAR license exception "Temporary exports-Tools of the Trade" (TMP) or Baggage (BAG).

The TMP License Exception provides that when laptops, PDAs and other digital storage devices (and related technology and software) are being used for professional purposes, returned within 12 months, kept under effective control of the exporter while abroad (i.e., kept in a hotel safe or other secured space or facility) and other security precautions are taken against unauthorized release of technology (i.e., use of secure connections, password systems, and personal firewalls), then the TMP License Exception might apply. The baggage (BAG) license exception covers personal items that are owed by the researcher and intended only for their personal use. These License Exceptions do not apply to Cuba, Iran, North Korea, Sudan, or Syria. You must contact the NDSU Export Control Officer before using either of these License Exceptions, as they are subject to record-keeping requirements.

Sharing Information While Traveling

You can freely take with you and exchange with anyone the results of fundamental research conducted on the NDSU campuses. However, if your work involves technical data controlled for defense of non-defense work a license from the Department of State may be required. Contact the NDSU Export Control Officer for more information.

Encryption – Publicly Available

NDSU does not provide encryption software on their computers or laptops. Within Windows 10 and Windows 7 there is a "bit locker" for full disc encryption; however, if you choose to utilize this option for encryption and you lose your password, NDSU staff will not be able to gain access to the encrypted material.

Countries that Restrict the Import of Encryption Products

Because encryption products can be used for illegal purposes many countries may ban or severely regulate the import and export of encryption products. The import of your laptop with encryption software to certain countries could violate the import regulations of the country to which you are traveling, and could result in your laptop being confiscated, fines, or in other penalties.

Encryption – Developed at NDSU

NDSU researchers, including faculty, staff and students, who are developing encryption software need to be aware of export control implications.

In most instances, encryption code developed at NDSU falls under the Fundamental Research Exclusion (FRE) and is not subject to export control laws and regulations. However, the FRE can be eroded if restrictions on the research exist. It is important that researchers make available any encryption code developed during the course of their research on a publicly-available website as quickly as possible. Access to the code should be open and not subject to login or password requirements. Failure to make the code publicly available in a timely way may trigger the application of export control laws, including restrictions on "deemed exports" to non-U.S. citizens within the U.S.

"Strong" Dual-Use Encryption Code

While most encryption code should be posted immediately to a publicly accessible website, researchers must inform an export control officer before making software available if it falls under the definition of "strong encryption software". Strong dual-use encryption, is defined in the Export Administration Regulations, Part 774, Commerce Control List, Category 5 (Part 2) Information Security at 5A002 (encrypted hardware) and 5D002 (encryption software).

The above content is offered as guidance to individuals. It is intended as a general overview of issues related to the export of encryption software and is not exhaustive. Questions about the application of export control regulations to specific situations should be directed to NDSU Export Control Officer.