University of Miami

Know Before You Go Travel Briefing: Research Security

Lory Hayes, Ph.D., CHRC,
Director, Disclosures & Scholarly Activities Management (DSAM)

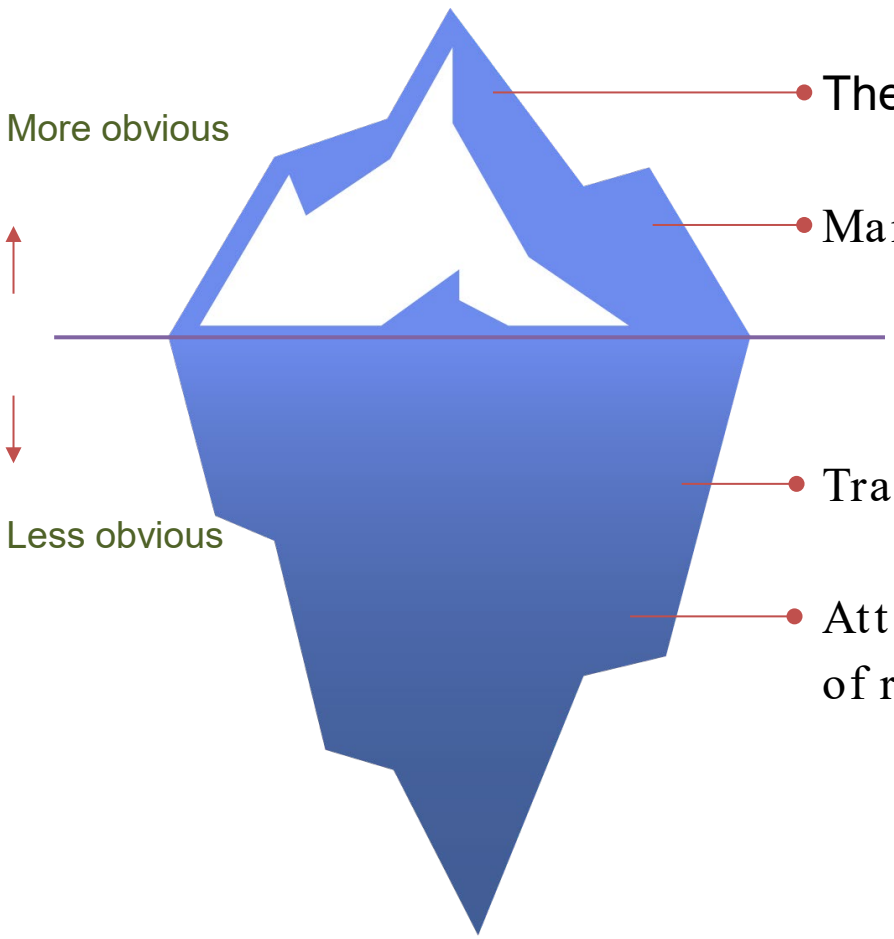
William (Bill) Collins,
Director, Export Control Compliance

What is Research Security?

"Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference."

NSF Office of the Chief of Research Security Strategy & Policy

Types of Research Security Issues



- Theft of data, IP, publications
- Manipulation of data
- Transnational repression
- Attempting to quash certain lines of research or shape the topic

Foreign Influence **is a malign intent to impact research**

Intention to slow down, reshape or halt certain lines of scientific or academic inquiry

UM's Research Security Program

UNIVERSITY OF MIAMI
OFFICE of the VICE PROVOST
for RESEARCH & SCHOLARSHIP

RSP

Export Control Training

✓

Cyber-security Program

✓

Research Security Training

✓

Foreign Travel Security

?

Transparency


What do Export Controls Affect at UM?
Restricted Sponsored Research
International Collaborations
International Visitors & Scholars
International Travel
Employing Foreign Nationals
International Shipping
Using Export Controlled Items
Distance Learning
Conducting Research Abroad
Procurement and Purchasing

What is an Export?

The federal definition of an export is any item that is sent from the U.S. to a foreign destination; to anyone outside the U.S., including U.S. citizens; to foreign entities, individuals, embassies or affiliates at any location, including the U.S.

Exporting may occur in any of the following ways:

- ☑ Parcel / Shipping
- ☑ Phone Calls
- ☑ eMails (including screen shots)
- ☑ Meetings (face-to-face / virtual)
- ☑ Auditory (eavesdropping)
- ☑ Lab Tours
- ☑ Electronically (Shared Drives, "cloud", Texting/SMS)
- ☑ Visually (instruction, observing)

"Items" include, but are not limited to, commodities, software or technology, retail software packages and technical information.

In a university situation, these items include, but are not limited to:

- ☞ unpublished research findings
- ☞ drones / UAV's
- ☞ lasers (high-energy)
- ☞ biological specimens / toxins
- ☞ computers (high-performance)
- ☞ sensors
- ☞ telecommunications (satellites, GPS, SONAR, underwater acoustics)
- ☞ funds/payments or services to restricted persons/entities (debarred, embargoed, etc.)

Who Is A U.S. Person?

U.S. Person (EAR Part 772 and ITAR 120.15)

Pursuant to the EAR and the ITAR, a U.S. Person includes :

- any individual who is **granted** U.S. citizenship; or
- any individual who is **granted** U.S. permanent residence ("**Green Card**" holder); or
- any individual who is **granted** status as a "protected person" under 8 U.S.C. 1324b(a)(3);
- any corporation/business/organization/group incorporated in the United States under U.S. law; any part of U.S. government.

Who Is A Foreign Person?

The regulations define a foreign person as anyone who is not a U.S. person.

Therefore, this includes :

- any individual who is **not** a U.S. citizen; or
- any individual who is **not** a US permanent resident alien ("green card" holder); or
- any individual who is **not** a protected individual (e.g., refugees, or have political asylum);
- any foreign corporation/business/organization/group not incorporated or organized under U.S. law;
- foreign government and any agency or subdivision of foreign governments (e.g. diplomatic missions). (BIS rules simplified the terms used in the EAR.)

If the individual is **not** a U.S person, when applying the "deemed export" rules the EAR looks at the person's most recent citizenship or permanent residence whereas the ITAR looks at the person's country of origin (i.e., country of birth) and all current citizenships.

The "deemed export" rule is an export (release) of controlled technology or source code to a foreign person who is in the United States.

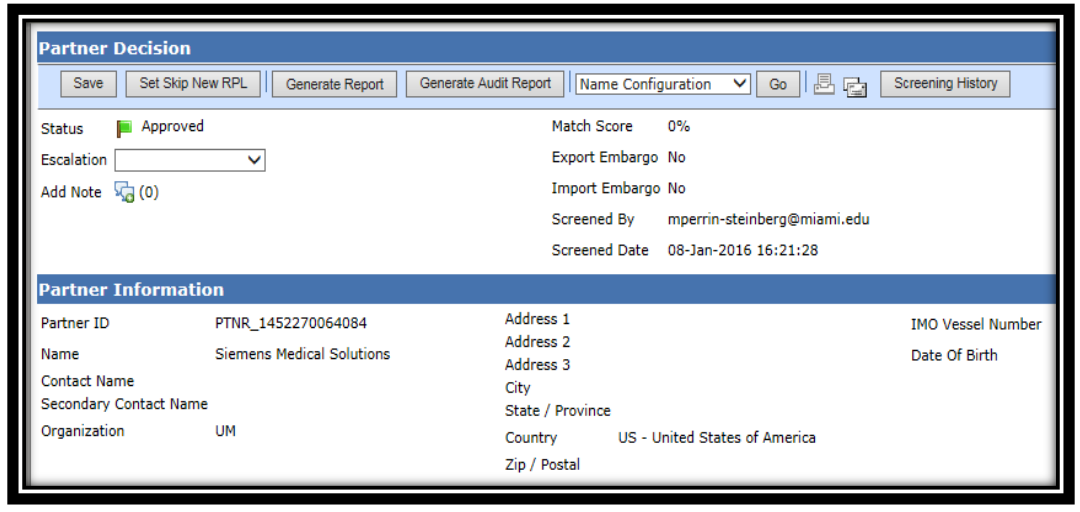
Restricted Party Screening (RPS)

Federal Regulations require that businesses and institutions "know their customer." One way to know our customer is to conduct a restricted party screening to ensure the individual or entity does not appear on any denied / restricted / debarred list.

RPS required for all foreign persons being sponsored by UM (I-129 / DS-2019); University purchases; University visitors; University research.

RPS is not the same as e-Verify, nor does it include local law enforcement records.

RPS system used by many offices / departments at UM to accomplish the necessary due diligence.



Any persons or entities that appear on any lists will likely be restricted from conducting business activities with the University.

License Exception (TMP) Temporary) and BAG (Baggage)

- When can License Exception TMP (Temporary) be used?
  - When travel is to a country on the Department of State list.
  - When encryption technology is not banned in the country.
  - When taking UM-owned devices that are considered Tools-of-Trade.
  - When the traveler will return to the U.S. within 12 months.
  - When traveler is a UM employee.
    - Justification for UM employees who are non-US persons must be provided and kept on file per regulations.

- When can License Exception BAG (Baggage) be used?
  - When travel is to a country on the Department of State list.
  - When encryption technology is not banned in the country.
  - When taking personally-owned devices that are considered Tools-of-Trade.
  - When the traveler will return to the U.S. within 12 months.
  - When traveler is U.S. Citizen, U.S. Permanent Resident or protected under asylum/refugee status.

- Some equipment that is used in research, such as GPS devices, thermal imaging cameras, inertial measurement units and specialty software do not qualify for use of License Exception TMP or BAG.

License Exception TMP Form (Temporary Export Tools of Trade)

International Travel Disclosure & Export Compliance Form

- Expanded version of UM's current TMP form
- Streamlines UM's requirements for international travel
- Collects information on streamlined sections:
  - Traveler Profile Information
  - Travel Details
  - Restricted Party Screening Request
  - International Collaborations
  - Export Control and License Exemption TMP Section
  - Traveler Attestation

Register Your Travel

UM's International Travel Approval policy states that to ensure proper safety procedures and insurance coverage, all international (foreign) travel must be registered with International SOS (iSOS) before departure and updated if there are any changes to the itinerary.

- **Automatic Registration**: Travel booked through UM's Travel Portal is automatically registered with iSOS.
- **Manual Registration**: Travel arranged outside the portal must be manually registered with iSOS, including any itinerary updates.
- **Traveler Responsibility**: Review iSOS guidance for their destination and take steps to ensure their own and their companions' health, safety, and security.
- **Registration Best Practice**: While not required for students or employees, registering with iSOS is strongly recommended.
- **Domestic Travel**: Faculty and staff are encouraged to register domestic travel to support Duty of Care.

Loaner Laptop Program

- Reach out to umit-procurement@miami.edu
- Submit the UM Academy Loaner Laptop Form
- Immediately report problems to UMIT Helpdesk at: 305-284-6565 or via e-mail at: help@miami.edu
- Provide details on your laptop/ UM-issued cell phone on the travel authorization form

How to clean devices

Follow these steps for institutional/personal devices you are taking with you:

Back up your data on an institutional cloud environment and/or external hard drive; leave the backup at home

Consider wiping devices to reduce compromise risk

Install the latest software and security updates on all devices because outdated software increases security risks

Forget all saved Wifi networks and Bluetooth devices

***Encryption and VPN are illegal and/or unavailable in some countries**

Set up your laptop:

- Remove any research data and IP (e.g., export-controlled, sensitive data) from local hard drive and store them in institutional cloud storage
- Use encryption* to protect your files
- Install institutional VPN* software

Set up your mobile devices:

- Turn on security/PIN codes (6+ characters) for your device's lock screen
- Install end-to-end encrypted messaging applications* (e.g., Signal, WhatsApp)
- Uninstall nonessential applications (e.g., social media)

UMIT: Protect Your Personal Information During Travel

What are elicitation attempts?

Elicitation (or foreign information collection) is used by various actors, including intelligence agencies, to **manipulate people into revealing information** that is not readily available or publicly known, such as trade secrets, personal information, or details about a person's work (i.e., research IP).

Pay attention to elicitation techniques:

- Subtle questioning
- Professional requests
- Exploiting expertise
- Flattery

Additional resources:

FBI Elicitation Guide

DCSA Elicitation Guide

Recognizing and Countering Elicitation

- **Be cautious when discussing your research during your travel!**
- **Be aware of the techniques** used in elicitation attempts:
  - Desire to help/appear knowledgeable
  - Leading questions
  - Building rapport
- **Be cautious of people who are overly eager** (e.g., probing for specifics), especially about **sensitive and/or unpublished information**
- **Be aware of your own tendencies** to want to be helpful, polite, or appear knowledgeable
- **Do not enter any agreements/collaborations** (verbal or written) with any individuals/entities/institutions

Cybersecurity Guidelines for International Travel

- **Don’t leave your laptop unattended** (locking in a hotel safe/room is ok in most destinations)
- Consider using **privacy screens** to prevent shoulder surfing.
- **Don’t use public USB power stations** (i.e., airport, hotel room)
- **Don’t allow others to plug devices**, such as USB sticks, into your devices
- **Don't auto-connect** to networks and avoid using public wifi
- **Follow institutional VPN requirements**
- **Follow institutional guidelines for accessing data** via cloud storage environments
- For mobile devices:
  - Turn off “join wireless networks automatically”
  - Always manually select the specific network you want to join
  - Turn off wireless and Bluetooth when not using these features (Airplane mode does not always disable Bluetooth)
  - Disable location services when not needed

Case Study

Russian-born researcher Kseniia Petrova was returning from France where she collected frog embryo samples for her lab.

U.S. Customs at Boston Logan Airport detained her after discovering the **undeclared biological materials in her luggage**.

Why is this important?

- Petrova claimed that she didn't know she was required to declare the samples.
- She was on personal travel to France when she picked up the samples.

Grand Jury Indicts Russian Scientist on Smuggling Charges

Kseniia Petrova, a Harvard researcher, was detained in February after failing to declare scientific samples she was carrying into the country.

Disclosure requirements

UM's Comprehensive COI Policy articulates that all *Covered Persons*, must

- Complete annual training (1st page of the disclosure form), and
- Disclose interests to UM on an annual basis, including:
  - Outside interests (including non-compensated business and fiduciary responsibilities, consulting, gifts, royalties, **travel**, etc.)
  - Financial interests of spouse and dependent children related to UM responsibilities
  - Non-UM *Scholarly Activities* (e.g., teaching & research)
  - Financial interests in entities that do, or propose to do business with UM
  - Receipt of non-UM, "Other Support," and
  - Foreign affiliations/income/support

- If any part of your trip is being paid for by a third party, it must be **disclosed** to UM

✓Disclosure and Research COI policy in PolicyStat

Key Takeaways

- When transiting any border, border agents may request to:
  - View your devices' messages, social media, photos, browsing history, and applications
  - Separate you from your device(s)

- Be aware that the government in some high-cyber risk countries control the internet (i.e., Russia, Saudi Arabia) and may attempt to remotely access your laptop to steal your IP or data.

- Even if you are not traveling to a country deemed high-risk, be aware that elicitation attempts are also common in third countries and situational awareness is always important.

- **Remove all research data and intellectual property that has not been published from your hard drive and store in a university cloud environment**

Who to contact?

What to disclose, elicitation attempts, or research security training?

Lory Hayes; lhayes@miami.edu

DSAM helpline: 305-243-0877

Email: DSAM@miami.edu

Export Control, TMP form, or restricted party screening?

Bill Collins; Wjc59@miami.edu

EC Office: 305-284-9558

Email: exportcontrol@miami.edu