



Foreign Travel Vulnerability Briefing

- **MUST** complete pre-travel briefing at least 15 days prior to departure date.
- ✓ Please review this brief and complete the highlighted Activities,
- ✓ Sign the completed document and email it to research.compliance@aamu.edu

AAMU-Travel Policy: <https://www.aamu.edu/about/policies-procedures/documents/research/3.4.1-international-travel.pdf>
Procedure: <https://www.aamu.edu/research-economic-development/research-compliance/foreign-travel.html>

Agenda

- Vulnerability Awareness
- Personal Safety
- Terrorist Threat Information
- Assistance Contacts
- Before You Go
- When You Return

Vulnerability Awareness

When traveling abroad, you must know how to protect yourself and safeguard your belongings.

In this section, you will learn about:

- How you may be a target
 - Counterintelligence
 - Collection techniques
 - Suspicious contacts
- Crime protection while traveling
- Foreign arrest and detention
 - Local laws
- Industrial espionage tactics

How You May Be a Target: What You Know

You may possess or have access to information that is highly sought after by foreign entities, including:

- Friendly information
- Research, development, testing, and evaluation
- Program milestones and specifications
- System capabilities

Foreign entities also target information related to your organization's personnel, security, and operations.

You are the first line of defense in protecting classified information and defense technologies!

How You May Be a Target: Counterintelligence (CI)

What is counterintelligence?

- Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against:
 - Espionage
 - Other intelligence activities
 - Sabotage
 - Assassinations
- Conducted by, for, or on behalf of:
 - Foreign powers
 - Foreign governmental and commercial organizations
 - Foreign persons or their agents
 - International terrorist organizations

How You May Be a Target: CI Awareness and Foreign Travel

Foreign travel increases the risk of foreign intelligence targeting.

- Collection techniques include, but are not limited to:
 - Bugged hotel rooms or airline cabins
 - Intercepts of email and fax transmissions
 - Tracking activity via ATM transactions and Internet usage at Internet kiosks and Wi-Fi access points
 - Recording of telephone conversations
 - Unauthorized access to or theft of electronic devices and installation of malicious software at customs or hotel
 - Intrusion into or search of hotel rooms and hotel room safes
 - Enhanced interviews by customs officials

How You May Be a Target: CI Awareness and Foreign Travel (cont.)

Foreign travel increases the risk of foreign intelligence targeting.

- Collection techniques include, but are not limited to:
 - “Honeytraps”
 - Suspicious approaches at public conveyances
 - Physical surveillance
 - Requests to transport items outside of the country
 - Exploiting criminal activities
 - Elicitation
 - Suspicious questioning by translators, guides, or cab drivers

How You May Be a Target: Identifying Suspicious Contacts

Examples of suspicious contacts include, but are not limited to:

- Requests for protected information under the guise of a price quote or purchase request, market survey, or other pretense
- Foreign entities targeting personnel travelling overseas via airport screening or hotel room incursions
- Attempts to entice personnel into situations that could lead to blackmail or extortion
- Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file
- Attempts to place personnel under obligation through special treatment, favors, gifts, or money

How You May Be a Target: What to Do if Approached

If you feel you are being solicited for information:

- Practice authorized responses to questions concerning your duties
- Never feel obligated to answer questions which make you feel uncomfortable
- If a conversation is too probing with respect to your duties, private life, and co-workers, change the subject
- Be observant and take note of the person questioning you
- Maintain professional composure
- **REPORT, REPORT, REPORT:** Provide as much information as possible to your security point of contact

Foreign Travel and Crime

Crime is one of the biggest threats facing travelers. Crimes against travelers are crimes of opportunity.

Follow these steps to protect yourself:

- Stay alert and exercise good judgment
- When possible, ensure your hotel room has a peephole and a deadbolt lock or a chain-and-slide bolt
- If you travel with valuables, put them in the hotel safe
- Find out what parts of town locals consider risky and avoid them
- Keep your car doors locked and suitcases out of sight
- If you see an accident, don't stop; instead, call for help from a safe area
- Minimize the amount of cash you carry
- Be wary of street vendors and innocent-looking youngsters as they may be decoys for pick pockets

Foreign Arrest and Detention

Foreign police and intelligence agencies detain persons for many reasons, including simple curiosity.

If you are detained or arrested for any reason:

- Exercise good judgment and be professional in your demeanor
- Stay calm, maintain your dignity, and do not do anything to provoke the arresting officer
- Ask to contact the U.S. Embassy or Consulate
- DO NOT admit to anything or volunteer any information
- DO NOT sign anything until the document is examined by an attorney or an embassy/consulate representative
- DO NOT accept anyone at face value: Request identification from embassy/consulate representatives
- DO NOT fall for the ruse of helping the ones who are detaining you in return for your release

Local Laws

While travelling, remember that you are subject to the local laws. Do not make assumptions about what is acceptable.

When travelling abroad:

- Be aware of local laws
- DO NOT photograph government facilities or religious symbols as it is prohibited in many countries
- DO NOT take photographs in the vicinity of foreign military bases, buildings, or personnel

Industrial Espionage

Industrial espionage: The acquisition of trade secrets from business competitors.

Tactics include, but are not limited to:

- Elicitation
- Eavesdropping
- Surveillance
- Electronic interception
- Hotel intrusions
- Theft of information
- Cyber exploitation

Personal Safety

New surroundings and exotic destinations may lead you into a false sense of security. Whether you are traveling for work or leisure, your personal safety is paramount.

In this section, you will learn about:

- Maintaining a low profile
- Hotel safety tips
- Travel safety tips

Maintaining a Low Profile

- Attempt to blend in with your surroundings
- Conceal material wealth
- Exchange your money into the local currency
- Drive an inconspicuous vehicle
- Use unmarked parking spaces and vary where you park
- Avoid publicity
- Only share information about your personal life and security efforts to trusted friends and security personnel
- Avoid establishing routines

Hotel Safety Tips

- Only patronize reputable hotels
- Note escape routes
- Secure your door and keep windows locked
- When away from your room, keep the television or radio on
- In high threat areas, avoid riding in elevators
- Avoid hotel paging
- Be aware that some countries require you to leave your passport with hotel reception over night so it may be checked by local authorities
- DO NOT stay in hotel rooms that are located on the first floor or easily accessible from the outside
- DO NOT accept deliveries unless previously arranged
- DO NOT leave your room key at the front desk; keep it with you
- DO NOT use the hotel phone to discuss travel plans

Travel Safety Tips

- Always remain alert and maintain a cautious attitude
- Walk toward traffic and in the middle of the sidewalk
- Don't wear clothing that immediately identifies you as an American
- Whenever possible, travel in groups
- Avoid public transportation (i.e., buses)
- Choose your own taxi
- Avoid isolated roads, danger areas, civil disturbances, and crowds
- Be alert to anyone who appears to be following you
- Have a working knowledge of the local language



Terrorist Threat

Acts of terror happen around the world. There are steps you can take to minimize the likelihood of being a victim to terrorist activity.

In this section, you will learn about:

- Terrorist tactics
- Threats to your travel destination

Terrorist Tactics

Terrorist tactics include, but are not limited to:

- Bombing
- Kidnapping
- Hostage-taking
- Hijacking
- Assassinations
- Arson
- Robbery
- Extortion
- Biological and chemical attacks
- Kinetic violence (e.g., stabbings, shootings, vehicular attacks)



Threats to Travel Destination

ACTIVITY 1:

Click the link below to search for your destination-specific threat information

- U.S. Department of State information:

<https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages.html>

- <https://travel.state.gov/>
 - Embassy and Consulate contacts
 - Travel alerts

Your Destination Country:

Travel Dates:

Departure

Return

Destination Threat Level:

Travel Alerts (if any):

Assistance Contacts

Even with the best preparations, things can go wrong. Know where to seek assistance should an emergency occur.

In this section, you will learn about:

- U.S. Embassy and Consulate contacts
- Domestic contacts

U.S. Embassy/Consulate Contact

ACTIVITY 2:

[Insert relevant embassy/consulate contact information for your destination country]

Domestic Contacts

ACTIVITY 3:

[Insert domestic contacts, such as:

- University point of contact
- Relatives/friends/colleagues]

In addition, make sure you have contacts for your:

- Financial institution
- Insurance company
- Family members

Before You Go

Your preparations will depend upon your destination and the trip's length and purpose.

Before you go:

- Make copies of your passport and other important documents
- Inform others of your itinerary
- Establish a point of contact for your family
- Know the local laws and customs
- Register your travel with the Department of State's **Smart Traveler Enrollment Program** (STEP) at step.state.gov to receive security & emergency alerts.
- Check health and immunization information with Center for Disease Control and World Health Organization
- Keep all medications in their original container

Organizational Policies

[AAMU's policies related to:

- Cybersecurity and use of virtual private networks (VPNs) while abroad]
- If you intend to connect to the campus network while on travel, please contact the AAMU-Information Technology Services (ITS) prior to your travel to setup a Virtual Private Network (VPN) to assure that your computer is in compliance with University regulations.
- Please note that ITS established a Laptop Loan Program which allows you to borrow a Secured Laptop that you can use while on international travel.



Additional Support

[U.S. Department of State](#)

[Central Intelligence Agency World Factbook](#)

[DCSA Reports, Flyers, Posters, and Handouts](#)

DCSA Center for Development of Security Excellence (CDSE)
Resources

- [Counterintelligence Awareness Toolkit](#)
- [FSO Toolkit](#)
- [Traveling with Mobile Devices](#)



When You Return

- Contact the Office of Research Compliance for a foreign travel debriefing upon return from your trip
- Report any suspicious activity or contact to your local security official

Acknowledgment

My signature certifies I have read and understand this Foreign Travel Briefing and can contact the Compliance Officer (CO) for clarification. I understand I MUST be briefed a minimum of 15 days PRIOR to departure and accomplish the following: Complete and return the Foreign Travel briefing to the CO/designee, register in STEP, and complete a travel debriefing within 5 business days of my return to the USA.

Traveler's Name

Traveler's Signature