

Student Guide

CI Foreign Travel Briefing Short

Introduction

The vacation of Joe's lifetime is right around the corner. He started planning this trip a year ago. The flight is booked, his accommodations are confirmed, and his passport is current. Everything is set. Or is it?

Is Joe aware of the current security threats for his travel destination? What about the threats to his industry? Does he have the necessary contact information in case he runs into trouble?

That's where you come in. A Foreign Travel Briefing will provide Joe with the answers to these questions and more.

Foreign Travel Brief

How do Joe and other travelers know what to watch out for while travelling abroad? Employees should complete a foreign travel briefing before departing on foreign travel. It is your responsibility to create and conduct this briefing.

The purpose is to: Increase awareness and personal safety while travelling internationally, increase the traveler's awareness of potential targeting by foreign intelligence, provide information on current travel warnings and alerts, and provide the traveler with information about where to seek assistance while traveling abroad.

Foreign Travel Brief Contents

To assist you in creating your own foreign travel briefing, let's review a sample. The briefing includes topics on vulnerability awareness, personal safety precautions, current terrorist threat information based upon the travel destination, who to contact if assistance is needed, and things to consider before the trip. These topics will prepare travelers for events they may encounter and arm them with the strategies needed to handle these events.

Vulnerability Awareness

In the Vulnerability Awareness section of the foreign travel briefing, you must inform personnel that when they travel overseas, they must be aware of the potential for danger.

This section discusses how travelers may be targeted and how to protect against crime while traveling. In addition, travelers must know what to do if they are placed under arrest or detained by foreign police or officials. Finally, travelers must also be aware of the potential for industrial espionage and tactics that may be used against them.

Personal Safety

In the Personal Safety section of the foreign travel briefing, you must inform personnel that it is important to maintain situational awareness.

This section covers strategies for maintaining a low profile while traveling abroad. It also includes hotel safety tips and the steps needed to safeguard possessions and maintain safe accommodations. Finally, overall travel safety should also be discussed.

Terrorist Threat

In the Terrorist Threat section, you must inform travelers that while they may not be able to mitigate being in the wrong place at the wrong time, there are steps they can take to minimize the threat of terrorism.

This section discusses terrorist tactics and threats specific to the traveler's destinations. Travelers must be aware that they may be targeted for being an American or even being affiliated with your organization.

Assistance Contacts

The Assistance Contacts section of the briefing should provide travelers with guidance needed to locate contact information for the local U.S. Embassy or consulate.

In addition to telephone and address, travelers should be aware of local landmarks so they may locate the U.S. Embassy in times of distress. Travelers should also maintain a list of domestic contacts. This includes contact information for their relatives, organization, financial institutions, physicians, and travel-related government agencies, such as the Department of State.

Before You Go

The Before You Go section assists travelers with travel preparations. For example, travelers should leave copies of their itineraries, passports and other important documents with family or colleagues.

Travelers should also be aware of their destination's local laws and customs. They should register their foreign travel online with the Department of State as a safeguard in case of natural disaster or other significant event. Finally, travelers should

research current health concerns related to their destination and the immunizations needed for travel.

Foreign Travel Debrief

When personnel return from foreign travel, you will conduct a debrief session with them. Depending upon the purpose and destination of the travel, this debrief may be as informal as a questionnaire or as formal as an interview. Regardless of format, the purpose is to determine if anything happened during the trip that raises a concern.

There are several content areas that are recommended. While this is not an exhaustive list of topics that could be covered, it is designed to guide the traveler to determine if and where any possible suspicious activity occurred. Take a moment to review the list of recommended topics:

- Countries and dates visited
- Irregularities at entry
- Gifts or provisions received
- Foreign inquiries
- Requests received
- Unexpected or unusual events
- Suspicious foreign contacts

Reporting Suspicious Activity

Personnel are required to report any suspicious foreign contacts and suspicious activity that occurs during foreign travel. Direct personnel to report to their local security contact. Reporting is essential so that threat information can be consolidated and larger threats may be identified.

Activity

You will now have the opportunity to create a CI Foreign Travel Brief for your organization or company. For this activity, Microsoft PowerPoint software needs to be installed on your computer.

From within the courseware, select the file "Foreign Travel Brief Template" to open a copy on your local machine. Then save a copy using the "Save " option. Now you are able to add in the information necessary for your personnel and their foreign travel plans.

The contents of the "Foreign Travel Brief Template" are included in Appendix A of this Student Guide.

Summary

Foreign travel briefings help prepare travelers for events they may encounter, and arm them with the strategies needed to handle these events.

You had the opportunity to modify a sample CI Foreign Travel briefing specific to your organization. This will help personnel in your organization when they travel abroad. The contents of the CI Foreign Travel briefing are included in Appendix A of this Student Guide.

The additional foreign travel information from the DSS CI Directorate is included in Appendix B of this Student Guide.

Appendix A:

Foreign Travel Brief Template

Foreign Travel Briefing

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

Vulnerability Awareness

When travelling 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
- Crime targeting foreign travelers
- Foreign arrest and detention
- 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!

Counterintelligence

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

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

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

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 that 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

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

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 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

Threats to Travel Destination

- Click to add destination-specific threat information
- U.S. Department of State information:
 - <http://travel.state.gov/>

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

- Click to add relevant embassy/consulate contact information, including surrounding landmarks

Domestic Contacts

Click to add domestic contacts, such as:

- Company point of contact
- Security point of contact
- Department of State contact
- Passport information or replacement contact

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:

- Inform others of your itinerary
- Know the local laws and customs
- Register your travel with the Department of State
- Check health and immunization information with Center for Disease Control and World Health Organization
- Establish a point of contact for your family
- Keep all medications in their original container
- Make copies of your passport and other important documents



Additional Support

- Contact your local security official for a Foreign Travel Debriefing upon return from your trip
- Report any suspicious activity or contact to your local security official

Appendix B:

Foreign Travel VULNERABILITY Brochure

CONSCIOUSNESS

vs. Carelessness



Whether the person, the information, or both are traveling overseas, information electronically transmitted over wires or airwaves is vulnerable to foreign intelligence services' interception and exploitation.

Many countries have sophisticated eavesdropping/ intercept technology and are capable of collecting information we want to protect, especially overseas.

Numerous foreign intelligence services target telephone and fax transmissions. Suspicious entities can easily intercept voice, fax, cellular, data, and video signals.

It is the conscientiousness or carelessness of the individuals responsible that determines whether or not our sensitive information is protected from unauthorized disclosure.



SECURITY Countermeasures

Some commonsense security countermeasures should include:

- Do not publicize travel plans and limit sharing of this information to people who need to know
- Conduct pre-travel security briefings
- Maintain control of sensitive information, media, and equipment. Do not pack these types of articles in checked baggage; carry them with you at all times. Do not leave them unattended in hotel rooms or stored in hotel safes
- Keep hotel room doors locked. Note how the room looks when you leave
- Limit sensitive discussions. Public areas are rarely suitable for discussion of sensitive information
- Do not use computer or fax equipment at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspect inquiries or conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely



Bottom Line:

Be Assertive. Be ALert. Be AwAre.

Report Suspicious Activity!

Report suspicious activity to your local security contact.
Your DSS point of contact is:

Foreign Travel VULNERABILITY



This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

FOREIGN TRAVEL

Favorite Tactics

Computer SECURITY



Foreign travel increases the risk of foreign intelligence targeting. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you, and their actions are not restricted within their own country's borders.

Collection techniques include:

- Bugged hotel rooms or airline cabins
- Intercepts of fax and email transmissions
- Recording of telephone calls/conversations
- Unauthorized access and downloading, including outright theft of hardware and software
- Installation of malicious software
- Intrusions into or searches of hotel rooms, briefcases, luggage, etc.
- Recruitment or substitution of flight attendants



Overseas travelers and the information in their possession are most vulnerable during transit.

Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside the hotel room) may be monitored and recorded.

Entities can analyze their recorded observations for collecting information or exploiting personal vulnerabilities (useful for targeting and possible recruitment approaches).

A favored tactic for industrial spies is to attend trade shows and conferences. This environment allows them to ask questions, including questions that might seem more suspect in a different environment. One assessment estimated that one in fifty people attending such events were there specifically to gather intelligence.



Cleared contractors provide critical research and support to programs giving the United States an economic, technological, and military advantage.

In a world where reliance on technology continues to grow, foreign entities have increased the targeting of electronic devices such as laptops, computers, and personal media such as Personal Digital Assistants and cell phones.

Travelers should report theft, unauthorized or attempted access, damage, and evidence of surreptitious entry of their portable electronics.

The following countermeasures can decrease or prevent the loss of sensitive information:

- Leave unnecessary electronic devices at home
- Use designated "travel laptops" that contain no sensitive information
- Use temporary email addresses not associated with your company
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Encrypt data, hard drives, and storage devices whenever possible
- Use complex passwords
- Enable login credentials on laptops and other devices

