

Traveling Outside the U.S.

The security and safety measures suggested here will help protect you from the loss of classified information and crime as well from terrorism. Some suggestions are more applicable to one form of threat than others. The level of risk varies from country to country and time to time, so you may need to pick and choose or modify the suggested security measures to meet your needs. These suggestions apply whether you are visiting abroad for business or pleasure or stationed abroad for a longer period.

It is strongly recommended that you register yourself and your family prior to traveling the US State Department Smart Traveler Enrollment Plan (STEP) located at: [STEP](#)

General

Obtain a pre-travel briefing from your security office, especially if you are traveling to a potentially dangerous or unfriendly area.



Check the Department of State and other current travel advisories regarding risks and local regulations in the country or countries where you will be traveling.

Report any suspicious activity or security incident during foreign travel to your security office or to the relevant U.S. Government agency.

Pre-Travel Preparations

Check your wallet. It should have a card identifying your blood type, known allergies, required medications, insurance company, and name of person to contact in case of emergency. Remove any credit cards and other items not needed during your trip. Remove anything that might cause you grief if a terrorist sees it, such as military or reserve documentation or humorous cards like the one that identifies you as an "Honorary Sheriff."

Make copies of your passport, air tickets, all credit cards you take with you, and any other documents to facilitate reporting loss and replacing them.

Some travelers prefer to conceal from casual observers that they are American and carry an American passport. They put a plain cover on their passport (covers available in stationery stores).

Carry-on luggage should contain a supply of any regularly taken prescription medicines (in original containers labeled with the pharmacy name and prescribing physician so they won't be mistaken for illegal drugs), an extra pair of eyeglasses, passport, and carefully chosen personal documents (copies only!).

If you are taking a laptop computer with you:

- Be sure the laptop battery is charged or that you have the power cord handy. You may be directed by airport security personnel to open and turn on your laptop to demonstrate that it is actually a functioning computer. If you can't turn your laptop on, you may not be permitted to take it on board the aircraft.
- If your laptop is new or relatively new, take with you some evidence of your ownership of the computer. This documentation should include the serial number. This is because U.S. Customs may try to impose an import tax if it thinks the computer was purchased abroad. Alternatively, you may register your laptop and any other valuables that might be mistaken as imports with U.S. Customs prior to leaving the country. You can do this at the Customs Entrance and Clearance Desk at the airport in advance of your flight.
- Be aware that some countries have import restrictions on laptops. Check before you leave to avoid delays and possible confiscation. Also some countries do not allow encryption of telecommunications traffic within their borders -- because they want to be able to monitor your messages. So plan any communications with your home office accordingly.

Use hard, lockable luggage. Be sure luggage tags contain your name, phone number, and full street address. It is best not to use a business card in a luggage tag, as it discloses your organizational affiliation. Use a closed name tag so that all personal information is concealed from casual observation. Do not display company logos on your luggage. If the luggage could open if dropped or mistreated by baggage handlers, run a strip of nylon filament tape around the suitcase to preclude its opening accidentally.

The locks on your luggage are not secure against the professional thief but can be a deterrent if the thief is in a hurry, as is often the case. For luggage and briefcases with two combination locks, set the combinations on each lock to different numbers. For luggage with a single combination lock, set the lock on each piece of luggage with a different combination.

To avoid inviting crime, plan to dress inconspicuously to blend into the international environment. Avoid the appearance of being wealthy. Consider taking and wearing no jewelry. If you choose to wear jewelry, turn rings around so the diamonds are not showing and avoid dangling earrings. Large, expensive-looking jewelry is an attractive target and dangling earrings are easily snatched.

Many people in poorer countries have the misconception that all Americans are wealthy. The less you fit that stereotype the better.

Know what dress is culturally acceptable in the country you are visiting. Some European and Middle Eastern countries frown on wearing shorts, especially when visiting holy sites. Why risk inciting someone with a grudge against the United States to take it out on you? You may also wish to avoid wearing any religious jewelry or symbols.

Consider obtaining a modest amount of foreign currency before you leave home. Criminals often watch for and target international travelers purchasing large amounts of foreign currency at airport banks and currency exchange windows.

Prepare yourself for all eventualities. It seems impossible, but consider what would happen if you became a victim of a hijacking, kidnapping, or other hostage situation. Are your personal affairs in order? How would you behave?

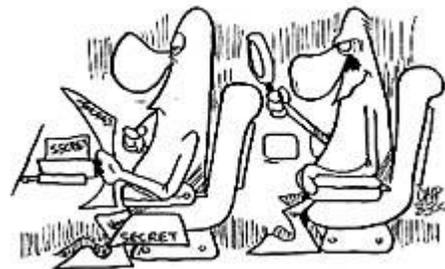
In Transit

Protect yourself against pickpockets, theft of laptop computer or camera equipment, and theft from train compartment. Watch for distractions that are intentionally staged to set up a pickpocket, luggage theft, or purse snatch (especially while passing through airport).

If carrying luggage, keep it within view or touch. When checking in at the airport, renting a car, or registering at the hotel, position your luggage against your leg and place a briefcase or a purse on the counter or desk in front of you.

At the airport, maintain a low profile. Do not delay in the main terminal area -- go through the security controls to the secure area as quickly as possible. If an incident occurs, take as much cover as possible behind a solid object such as a pillar or stairwell.

The airplane is not an appropriate place to discuss sensitive subjects. Conversations can be overheard and papers read by unauthorized persons. The national airline of at least one friendly foreign country is known to collect intelligence by bugging the seats of passengers, especially passengers in first class or business class.



Do not discuss or work with sensitive information in an airplane.

If you use your laptop while flying, be aware that other passengers may be looking at more than just the in-flight movie. A survey of 600 American travelers found that over one-third admitted looking at someone else's laptop while flying. Younger travelers were the worst offenders, with 49 percent of the men and 40 percent of the women under 40 admitting they look at what their seatmate is working on. Most are checking to see *what* their fellow passenger is doing, while others are more interested in *who* they are working for.[1](#)

On foreign airlines, avoid speaking English as much as possible. If your plane is hijacked, do not try to cover up the fact that you are an American citizen or in the military. Never volunteer this information, but, if a hijacker finds out that you have attempted to conceal your identity, the consequences could be worse than if you had cooperated from the beginning.

At the Hotel



Foreign security services have well-established contacts with hotels that commonly host conferences and meetings with international participation. Some even have their own office within the largest hotels. If the local intelligence service considers you a significant intelligence target, you are likely to be assigned a room that is equipped to monitor your in-room conversations and phone calls. To avoid this, it may help to make your own room reservation in a smaller hotel less frequented by foreigners.

If possible, stay with your luggage until it is brought into the lobby or placed into the taxi or limo. Consider using the bellhop, as luggage in the "care, custody and control" of the hotel causes the hotel to be liable for your property.

As you check in, be aware of persons in the hotel lobby who may have unusual interest in your arrival.

In many countries, you will be asked to surrender your passport when registering at a hotel. This is a routine procedure, as hotels must submit a daily report to police on all registered guests. Although a routine police procedure, be aware that this information may also be reviewed by a local intelligence service looking for targets of opportunity. Don't forget to get your passport back at the earliest possible time.

Use all the locking devices on your room door. Check locks on any sliding glass doors, windows, or connecting room doors. Remember that the hotel's emergency keys can override deadbolt locks.

Don't advertise to others when you are out of your room. For example, request housekeeping to make up your room while you are at breakfast, rather than leave a "Please Service This Room" sign on the door knob. When you are out, put the

"Do Not Disturb" sign on your door to give the impression that the room is occupied. Consider leaving the light or TV on when you are out of the room.

Carry the room key with you at all times instead of leaving it at the front desk. Do not needlessly display guest room keys in public or carelessly leave them on restaurant tables, at the swimming pool, or other places where someone can easily steal them. Do not use your name when answering the phone.

Do not accept packages or open the door to workmen or any other unknown person without verification from the front desk. If a person claims to be an employee, call the front desk and ask if someone from their staff is supposed to have access to your room and for what purposes.

Keep your luggage locked whenever you are out of the room. It will not stop or hardly even delay the professional thief or intelligence agent, but it will keep the curious maid honest.

At night, lock your passport and other valuables (including laptop computer and camera) in your luggage or room safe. This reduces the risk of their "mysterious" disappearance while you are asleep or in the shower.

Any papers, diskettes, or other materials that would be of value to a foreign intelligence service should be kept on your person at all times. They should not be left in a hotel room, in the hotel room safe, or in the hotel's safe deposit box.

Valuables such as money, jewelry, camera, credit cards, airplane tickets, or passport should be kept in the room safe or hotel safe deposit box when not needed. Note that the hotel is not responsible for items left in a room safe. It is responsible for items left in the hotel safe deposit box or main hotel safe where it is in the "care, custody, and control" of the hotel.

You can gain some additional security for papers and valuables left in a safe by putting them in one envelope inside another envelope. On the inner envelope, write your initials across all seams and then tape over all seams and edges.

Do not invite strangers to your room.

In some areas it is a good idea to carry a flashlight with you. Emergency power sources and emergency lighting often do not exist in hotels in the developing countries.

Street Crime

Attempt to travel in pairs or with others when possible.

Know the local currency. Fumbling with a wad of unfamiliar bills highlights you to any potential thief. Keep small and large bills separate so you don't pull out a wad of large bills when paying for a cup of coffee. Keep some small bills handy in a front pocket to hand over to a mugger. It is a good idea to keep your wallet in a front pocket to make it more difficult for a pickpocket. Inspect your credit card after using it to ensure it is yours. The credit card exchange scam is not new.

Never resist armed robbery; it could lead to violence. Always carry some cash to appease muggers who may resort to violence at finding no reward for their efforts. Turn over the small bills that you keep separate for this purpose. If the thief presses the attack, give up your wallet. If you do not have much money on you, offer something else. "I don't have my wallet; here, take my jacket." Never pursue a thief. Call for help and contact the police.

When walking, do not take shortcuts through alleys or off the beaten path. Try not to walk alone. If alone, be back in the hotel by dark. Pre-plan your route. On the street, walk confidently and try to avoid walking alone. Walk in the middle of the sidewalk. In many countries on the African continent and in several former East Bloc countries, there has been an unparalleled increase in violent street crime.

When driving, pre-plan your route. Get information on the area you are visiting. Check the area before you get out of your car. Avoid parking in unlighted lots that require you to walk any distance along dark streets.

If you are taking public transportation, have your destination address written out in the local language on a piece of paper, if possible. Choose a subway stop that affords easy, well-lit access to your destination. It is better to walk a few extra well-lit, well-traveled blocks than to cut across potentially hazardous areas. Check the area before you depart from public transportation.

Know how to work the local public telephones. Memorize or write down emergency phone numbers and carry change for phone calls.

To avoid marking yourself as a potential target, rent a conservative automobile. In Central America and Africa, one of the hottest crime waves is carjacking. The carjackers frequently target upscale sport utility vehicles and quite often are very violent. Avoid getting boxed in by other vehicles; leave an avenue of escape open should the need arise. If you have a good opportunity, don't be afraid to floor it and get away quickly if your life seems threatened.

Protecting Sensitive Information

Keep all sensitive documents in your personal possession and physical control at all times.

Hotel rooms and restaurants are rarely suitable places for sensitive discussions. If possible, conduct sensitive discussions outdoors in a spot where you are not vulnerable to bugging and conversations cannot be overheard.

Recognize that your laptop computer is a major target for theft. If you must take it, always keep it as carry-on baggage – never check it with other luggage. Leaving it in your hotel room also presents a significant risk. Lock it in your suitcase so it is out of sight while you are out of the room or asleep at night. If possible, copy sensitive material to a diskette and delete it from the hard drive prior to travel. Carry the diskette on your person, separate from the computer.

If secure communications equipment is accessible, use it for any discussion of sensitive matters. Do not use computer or fax facilities at foreign hotels or businesses for sensitive matters.

Protect unwanted sensitive material until it can be disposed of securely – by burning or cross-cut shredding. Cut floppy disks into small pieces.

Beware of new acquaintances who probe for information about you or your work or who attempt to get you involved in what could become a compromising situation.

In Case of Civil Unrest

Common sense tells us to avoid street demonstrations. If you are overtaken by a demonstration, seek refuge in the nearest safe haven such as a large hotel or department store. Choose your safe haven carefully. If there is an anti-American demonstration, trying to make your way through the crowd to get inside the local office of a prominent American corporation is probably a bad idea. Do not try to make your way out of the area by subway. You may be stranded in a crowded underground station if local authorities stop service to that particular station because of the demonstration. Also, tear gas is heavier than air and fills up low lying areas like subway stations.

In the event of a major civil disorder, stay in your hotel. Do not watch activity from your window. An inside room provides greater protection from gunfire, rocks, grenades, etc. If others may have concerns about your safety, or if emergency evacuation may be required, advise the U.S. Embassy or Consulate or other friendly embassy of your status and location. Hire someone to take a note to them if phones are out of order.

Avoiding and Recognizing Foreign Intelligence Interest

While traveling abroad, you are on the other country's home turf where the local security and intelligence services have many resources available. They can monitor and, to some extent, control the environment in which you live and work. You, in turn, may be at a disadvantage, because you are on unfamiliar territory.



Allied as well as hostile intelligence and security organizations use their home field advantage to look for potential sources who can be developed and exploited based on greed, manipulation of psychological or emotional weaknesses, conflicting loyalties, addiction, or coercion. The local services routinely monitor black market activities, dissident groups, prostitution, certain bars, gay hangouts, gambling establishments, and other areas where human weaknesses may be observable.

Many Americans possess personality traits that increase their vulnerability to the classic routines of espionage.

- Sociability: Americans characteristically want to be liked. In order to gain approval we tend to be social and gregarious even with casual contacts.
- Candor and Trust: Americans generally place a high value on candor and on trust. We tend to be open and trustful and to accept others at face value.
- Pride: As Americans, we are proud of our phenomenal accomplishments in science, business, war, and world leadership. We tend to underestimate people from other cultures, including their ability to conduct successful intelligence operations against us.
- Ambition: Americans tend to be ambitious, oriented toward job advancement and professional recognition. Success is often measured by money and status.

These personality traits make many of us vulnerable to manipulation by people who offer friendship, understanding and flattery, or who offer opportunities for money or professional recognition, but who may have an ulterior motive for doing so.

Avoiding Intelligence Interest

To eliminate, or at least reduce, the possibility of your doing something inadvertent that may mark you as a person of special interest to one of these agencies, here are some *DO NOT*'s to remember:

- DO NOT do anything which might be misconstrued or reflect poorly on your personal judgment, professional demeanor, or be embarrassing to you, your employer, or your country.
- DO NOT gossip about character flaws, financial problems, emotional relationships or marital difficulties of any co-workers, or yourself. This type of information is eagerly sought after by those who would like to exploit you or another employee.
- DO NOT carry, use, or purchase any narcotics, marijuana, or other abused drugs. Some countries have very stringent laws covering the import or use of medications and other substances. If you are using a prescribed medication that contains any narcotic substance or other medication that is subject to abuse, such as amphetamines or tranquilizers, carry a copy of the doctor's prescription for all medications and check for local restrictions and requirements prior to departure. Some countries may require additional documentation/certification from your doctor.
- DO NOT let a friendly ambiance and alcohol override your good sense and capacity when it comes to social drinking. In some countries, heavy drinking in the form of toasting is quite common, and very few westerners can keep up with a local national when it comes to drinking the national brew. If you are not careful, you could easily embarrass yourself, your employer, and/or your country. An accident while driving under the influence could lead to serious trouble.
- DO NOT engage in "black market" activities such as the illegal exchange of currency, or the purchase of religious icons or other local antiquities that may be stolen or otherwise not authorized for export.
- DO NOT accept or deliver letters, packages or anything else from or to anyone you do not know. You have no way of knowing what you are carrying and it could result in your being arrested for illegally importing a prohibited item.
- DO NOT engage in any type of political or religious activity, or carry any political or religious tracts or brochures, or publications likely to be offensive in the host country, such as pornography or weapons.
- DO NOT photograph anything that appears to be associated with the military or internal security of the country, including airports, ports, or restricted areas such as military installations.

- DO NOT ask the local government for any special favors or permits, such as permission to travel to a restricted area or a special benefit for a relative or friend.
- If in doubt, DO NOT.

Recognizing Intelligence Interest

Several scenarios that are particularly common while traveling abroad are mentioned here. The following situations should be closely scrutinized and usually avoided, if possible.

- Repeated contacts with a local or third country national who is not involved in the business or other purpose of your visit, but who appears at each social or business function to which you are invited. This individual's demeanor may indicate more than just a passing interest in you or your work.
- A close personal and social relationship with a foreign national of a hostile host government is often unavoidable for business reasons. In these instances, don't let your guard down. Don't assume that this is a true friendship.
- Be skeptical of the accidental encounter with an unknown local national who strikes up a conversation and wants to practice English, talk about your country or your employment, buy you a drink because they have taken a liking to you, talk to you about politics, or who uses any other pretext to begin a "friendly" relationship.

If any of the above or anything else occurs which just does not ring true, be skeptical! It may be innocent, but exercise prudence and good judgment.

If you become aware that you are under physical or technical surveillance, this is a strong indication that someone is interested in monitoring your activities and learning more about you. Physical surveillance refers to following you on foot or by car. Technical surveillance refers to bugging your hotel room, using a concealed camera to observe your behavior in your hotel room, or monitoring your phone calls.

Although obviously worrisome, surveillance is no cause for panic. It may be a routine search for information that can be used against you, initiated solely on the basis of the sensitive information to which you are presumed to have access. You may be followed only because you met with someone who happens to be under surveillance. The bug in your hotel room may be left over from a previous

operation, or be a permanent installation that is activated only when the room is occupied by a more important target than you.

If you possess sensitive information, either in your head or in documents on your person, you should ASSUME that you may be followed and behave accordingly. Do not do or say anything that could be used against you or that might increase interest in you as a target. Although you should be alert at all times, DO NOT do anything that suggests you are either looking for or are trying to avoid surveillance. This would suggest that you are engaged in illegal or improper activities and make you an even more important target.

In your hotel room, ASSUME that the room and telephone are being monitored. DO NOT try to play investigator and start looking for electronic listening devices. This again could send the wrong signal to whoever is behind the surveillance. Just act normally and make sure that you do not say or do anything in your hotel room that you would not want to see printed on the front page of the local newspaper. And do not do or say anything that suggests you know or suspect someone is listening. Taunting the local security service is always wrong, as it is definitely counterproductive.

If you have any reason to believe that you are being targeted by an intelligence or security service or any criminal or terrorist group, there is only one course of action to follow. Report your suspicions to the American Embassy or Consulate or to your employer and follow their guidance. Report only to an American citizen, not to a local national. And report only in person, not by telephone, fax, or electronic mail, as such communications to the American Embassy or Consulate may be monitored.

Should you have questions, please contact the FSO at seandoyle@erc-incorporated.com or 256-327-9155.