Executive Travel Security

Executive & Corporate Travel Security Strategies

Revision Date: July 2009
The Executive Traveler
A Defensive Travel Program

Each year, thousands of U.S. business executives travel abroad either for business or pleasure. For most executives, foreign travel appears to be a positive, rewarding experience. For the few who experience security or safety-related problems, a lack of planning and general awareness are often contributing factors. For those same executives, the bad experience may have seemed a random incident when in actuality it was a targeted effort against the individual or company. Any executive traveling overseas should take their personal safety and security seriously, as well as the safety and security of their business information. While personal safety is paramount, the bad experience may not be a threat to safety, but a targeted effort to collect competitive intelligence on a company. Good security habits will not detract from travel and will only serve to enhance it.

This booklet contains information to assist an organization in designing or improving an internal executive travel program, as well as security reminders to help executives avoid pitfalls while traveling overseas. It is not a substitute for a Defensive Travel Briefing, which all executives should receive from appropriate security or risk management personnel in their organization. Such briefings will contain current security considerations for a destination as well as an overview of the company’s critical information that needs to be protected while traveling.

The first part of this booklet provides protective strategies and case studies security managers can incorporate into their travel security programs. The second part provides specific information for the traveler to protect themselves, corporate information and corporate technologies while abroad.
Upon returning to his hotel, an American executive in Paris surprised two men in his room. The two, carrying what appeared to be electronic equipment, said they were there to repair the window. They left immediately, and the American discovered that his briefcase had been searched. The traveler then took the obvious and appropriate action. He reported the incident to his security department. Unfortunately, his response is an exception! Most travelers either don't recognize the operations of foreign intelligence services focused on them or choose not to report those incidents they recognize as suspicious.
PART I

EXECUTIVE & CORPORATE SECURITY STRATEGIES

Any company that engages in global commerce should have a travel security program designed to protect the traveler as well as the organization. This section discusses the four components of an executive security program and provides protective strategies for the traveler. The term “Executive” in this booklet refers to anyone within an organization that has access to, or knowledge of critical information within an organization. Therefore, an executive, engineer, systems administrator, or other person with intimate knowledge of the organization is the intended audience of this awareness training.

The FBI prepared this booklet to inform American travelers of their vulnerability to foreign intelligence service operations and to elicit cooperation in reporting suspicious events. As Stan Levchenko, a former KGB intelligence officer and noted counterintelligence lecturer succinctly stated “...the most effective tool against the KGB in this country is public awareness of its methods of operation.” More importantly, public awareness is a significant deterrent to the activities of any intelligence service or corporate espionage effort.

EXECUTIVE TRAVEL SECURITY PROGRAM

An Executive Travel Security Program should be a formalized process to analyze the travels of an organization’s key personnel. The process consists of four stages: assessment; planning; countermeasures; and reporting. Organizations that fail to formalize this process risk their organizations' proprietary information and technology, as well as their position in overseas negotiations. The four components (stages) of an Executive Travel Security Program are listed below:

1. COUNTRY ASSESSMENT & RISK ANALYSIS: When foreign travel is being contemplated for key individuals in an organization, an assessment should be made of the destination. The assessment should include the purpose (value) of the travel, the current political and safety conditions of the destination country, and the potential risks to the traveler and the organization. Once these variables are identified, a risk analysis should be conducted to mitigate risks and possibly offer alternatives. Alternatives may include canceling the travel, having all parties travel to a third country, have parties travel to the U.S., implement secure technologies to conduct virtual meetings.

2. PRE-TRAVEL PLANNING & CONTINGENCIES: Once travel has been deemed necessary, the next stage should be the evaluation of the travel plans. Exactly where in a country will the executive travel: country; region; city; roadways; airports; hotels; meeting locations. All these locations pose differing security and safety concerns. Planning will involve everything from general security precautions and training, to overseas workers and translators, to social and political unrest issues, to natural disaster and pandemic considerations. Contingency planning should consider procedures to deal with hostage situations, natural disasters, country evacuations, missing traveler, bodyguards, etc. Additionally, a personal risk assessment for all personnel traveling should be conducted on the individual traveler. This personal risk assessment
will determine if there are any issues with personal affiliations or ethnicity that may increase risk to a travel destination.

3. TRAVEL PROTECTIVE STRATEGIES: Protective strategies are specific countermeasures executives and organizations implement to protect sensitive and critical information from compromise. These strategies are awareness issues as well as technical measures.

4. POST TRAVEL ASSESSMENT: Once the executive returns from overseas travel, a travel debriefing is conducted to identify potential compromises, or attempts at compromise of critical information. This assessment will also collect information regarding unusual circumstances or noteworthy incidents. These post travel debriefing should be used to further improve and evaluate the Executive Travel Security Program.

CRITICAL INFORMATION & TECHNOLOGY
It is essential that every organization identify critical information and technologies and inform executives and key personnel what must be protected. Critical information & technologies may include:

- customer data
- employee data
- vendor information
- pricing strategies
- formulas and processes
- technical components & plans
- corporate strategies
- corporate financial data
- computer access and design
- proprietary processes
- acquisition strategies
- marketing strategies
- investment data
- negotiation strategies
- passwords (computer, phone, accounts)
- phone directories
- other data of concern

TRAVEL PROTECTIVE STRATEGIES
One of the most serious threats facing the executive traveler is corporate espionage. The perpetrator of this type of espionage can be a competitor, opportunist, or foreign intelligence officer. If your company handles information or technology that may impact national security, the FBI can assist in providing additional protective strategies not included in this booklet. It is important to understand that in many countries, corporations may be partly or wholly owned by the government. These situations are exceptionally risky when the foreign government considers the company or industry important; it can utilize government resources (intelligence services, customs official) to collect competitive intelligence.

Following are a list of recommended personal, technical and post travel recommendations and strategies organizations should consider for inclusion in their travel security program and briefings.
PERSONAL PROTECTIVE STRATEGIES

Two American female students attended classes in what was then East Germany. On one occasion, they discussed, privately in their apartment, the lighting in their apartment. The next day, a light that had been out for weeks was working. In another incident, their room was burglarized and their passports, credit cards, and other personal, identification taken.

Personal Information Protection

- Do not travel with information that reveals your personal interests, hobbies, affiliations, loyalties. During an official or covert search, this information may be noted and later used for manipulation, especially during negotiations.
- Sanitize information you carry to eliminate possible negative affiliations. Searches conducted during violent situations such as hostage taking, rebel checkpoints, or a coupe situation may reveal your affiliations to an opposing party or position. (In one terrorist hostage situation, all wallets were searched and military identification was found. The individuals were beaten and one was killed.)
- Sanitize information you carry to reduce compromise of company systems. Do not carry passwords to company systems, voicemail, email accounts, customers systems. If you must carry this data, carry it on your person at all times. If it leaves your possession have a plan to reissue new passwords.
- Sanitize information you carry to ensure no critical information (printed materials, disk drives, and electronic data) is in your possession that is not necessary for travel. If critical information is necessary, take measures to ensure the material is on your person at all times, encrypted or otherwise protected. Hotel safes are not adequate to protect against foreign government corporate espionage.
- Consider any information or electronic component that leaves your possession and visual control for more that two minutes likely compromised (copied, downloaded).

An American salesman, visiting Moscow, was carrying product samples for the Russians and planned to present a paper at a symposium. The samples and his presentation were stolen from his hotel room. Later, he traveled to a factory in Leningrad where he saw his samples in the possession of a Russian scientist.

Targeting Techniques

- Be aware of ethnic targeting. Individuals of the same ethnicity as the destination country may be targeted based on their cultural or family ties to the country. Be aware of discussions requesting information on your heritage, loyalty, and family.
- Beware of offers to privately consult (outside of company parameters) while overseas. Doing so may violate U.S. deemed export laws. In addition, it may be an attempt to develop a confidential relationship with you.
- Exhibitions, conferences, and symposiums are opportunities for individuals to elicit information regarding your personal interests, corporate programs, and technical knowledge. These forums are used to spot and assess individuals of interest.
- Because of your position or influence within an organization, industry, U.S. government, or the international community, you may be targeted for a perception management campaign where
your perceptions and positions are manipulated so you become an unintentional promoter of a foreign interest. These techniques are as simple as developing a close, meaningful friendship with someone (who has an hidden agenda) or being provided an exceptional experience that skews your perception. These campaigns can be long-term, many months or years. You would in effect become an unknowing Agent of Influence for a foreign entity or government.

- Joint venture and mergers pose a particularly dangerous position for companies especially when a company has to reveal sensitive information during the process. Deals overseas require a significant amount of corporate information to complete and are often carried overseas or sent electronically. This information may be compromised before you even sit down to negotiate.

*An American in China was given a letter by a man he had never met. He tried to return the letter but the man ran away. That evening Chinese security officers visited the American, admonished him for taking the letter, and required him to sign a statement concerning the event.*

*A female military officer visiting Leningrad as a member of a tour group was told by a Russian, who spoke perfect English, where she could buy black market items in the hotel. Although she did not visit the room, she mentioned other Americans, both military and civilian, did.*

*On three separate occasions, a businessman, staying in China, was offered complimentary massages by attractive Chinese women who knocked at his hotel room door.*

Compromising Situations

- You may unwittingly become embroiled in a compromising situation. These situations can be planned, or an incident of opportunity for a foreign entity. The foreign entity or government may offer to intervene on your behalf and there will be an understanding (sometimes unstated) of your indebtedness.
- Many countries have serious counterfeiting problems. It's recommended you utilize respected banks and hotels for exchanges. Obtain small bills. Using large bills may cause you to receive counterfeit bills in change. Taxis and restaurants are known to engage in this scam. Possession of counterfeit bills may cause you to be the subject of an investigation or detention.
- Avoid street gatherings and protests. Sometimes police arrest individuals in roundups.
- Avoid religious settings and gatherings (in countries where tensions exist).
- Avoid political gatherings and public support of political parties.
- Avoid parts of a town where you could be targeted for scams. Scams may include false accusations.
- Avoid traveling alone or allowing members of your group to travel alone. Alone, a person may be more vulnerable to agree to a deal to escape a compromising situation.
- Avoid the *Honey-Pot*, which is an enticing romantic or sexual offer that is difficult to refuse. The offer will most likely occur in a social encounter not an obvious sex for money situation. At some point, the situation becomes compromised when the person turns out to be underage, claims rape, or a spouse appears.
Always check your bags. Items could be placed in them at anytime that could lead to your arrest. Items include drugs, large sums of money, political material, government information, pornography, artifacts.

Do not take photographs of military installations, checkpoints, government facilities, and police and military operations. Photographing such items may be illegal and lead to your arrest.

Do not carry or produce any anti-government material (buttons, posters, slogans, pictures).

An American government contractor staying in a Beijing, China hotel mentioned, privately in his room, that a light was not working in his closet. The next day the light bulb was replaced. The American also observed an elderly couple in the room next-door. The couple stayed in the short-term, expensive hotel room for his entire stay (several weeks) rarely leaving the premises.

An American business executive traveling to China to attend a conference returned to his hotel one evening. He was approached by a Chinese female who asked him the time and tried to engage in conversation. Her nervousness alerted the man who ended the encounter. As he walked down the hallway on his floor, two males exited what appeared to be the businessman’s room. They hurried down the hall, past the man, carrying a bag and keeping their heads down. In his room, the man observed his laptop case was hastily shoved back under his bed with the power cord protruding. The laptop would not turn on and the company’s computer department later determined the computer had been physically and technically compromised.

TECHNICAL STRATEGIES

- Sanitize laptop computers to remove any critical company information. Disable dial-in or web access programs that link to company networks. If a connection is necessary, consider appropriate protections such as encrypted connections. If critical electronic information is necessary during a trip, consider a removable hard drive or an encrypted thumb drive to keep on your person at all times. Emails, non-essential reports, password files, internet histories, internet cookies, and system access instructions should all be removed from computers.
- Company laptops can be cloned prior to travel. Upon return, the laptop and clone are compared to see if any additional programs or data were installed. This technique is used to detect malware.
- If your computer is out of visual range for more than two-three minutes, consider the system compromised. The system may have malicious software, spy software, or a listening devise implanted.
- Avoid using non-company computers to log into company network or website. Always consider any information conveyed through a non-company computer compromised by the foreign entity or government even if encrypted. Encryption and strong passwords are no defense against screen capture programs and key loggers.
- Clean out your voice mail prior to travel. Avoid sensitive messages being left in your voicemail during your travel. When you access your messages, the pass code may be compromised and others may retrieve those same messages. Your information management team may be able to monitor your access to see if additional attempts are recorded. Always change your voice mail pass code upon return from overseas travel.
- Sanitize cell phones and PDAs. These devices may contain email, voice mails, personal and company photographs, documents, and system passwords.
• Sanitize company camera and disks to ensure there are no photographs revealing business strategies or technologies. An example is a photograph of new a product line, manufacturing system, or company of interest in a pending merger or acquisition.

• Electronic eavesdropping has been reported on overseas airlines seats, hotel rooms, taxicabs and meeting rooms. Discussing business and negotiation strategies with coworkers is very difficult overseas and should be handled carefully and thoughtfully, or avoided. Raising the television volume in a hotel is not an effective strategy to neutralize electronic eavesdropping.

• If travelers must log into systems and voicemail, have traveler note access times and duration for comparison to company logs. (Discussed further in Post Travel action below.)

• 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 communications. So plan any communications with your home office accordingly.

*While a student in Moscow, an American had an affair with a Russian. Eight years later, the American who has become a government employee, received a letter from the Russian, in flawless English, offering to renew their "special relation."*

POST TRAVEL

• Upon return from overseas travel change passwords and access codes on company network, email, phone mail, and personal information accounts.

• Your organization’s Information Security Officer should review with you your system access during your travel. Access that was not accounted for should be investigated and a damage assessment conducted.

• The organization’s Security Officer should conduct a Post Travel Debrief with traveler. Be sure to report any unusual circumstances or noteworthy incidents to your Security Officer and/or the FBI upon your return. Your Security Officer ensures that other travelers from your organization are aware of the general security precautions, as well additional threats you report. Notifying the FBI will help to ensure the FBI travel briefs and the official U.S. Department of State Travel Advisories take into consideration any unusual circumstances or noteworthy incidents you encountered during your travel.

• If a suspicious contact or social encounter is identified, an additional future debriefing should be planned to identify/assess post travel contacts.

• If a compromise is suspected or confirmed, a damage assessment should be conducted that details the extent of damage and vulnerabilities. Countermeasures must be implemented to reduce the risk of a similar compromise in the future.
PART II

PERSONAL SECURITY STRATEGIES

BEFORE YOU GO
The preparations you make before you depart for your trip will depend upon the destination, length, and purpose of your travel. Before leaving, be sure to confirm lodging and travel reservations and obtain traveler’s checks. Unless anonymity is an issue, also leave a copy of your itinerary with a relative or close friend. You should take with you pertinent information regarding health insurance coverage which might be useful in an emergency. In addition, you will need certain official documents and perhaps vaccination information for some areas. The following page contains a checklist which will help you prepare for your trip.

CHECKLIST

- Learn about the places you plan to visit. Familiarize yourself with local laws and customs in those areas. Information can be obtained from your public library, local travel agency or the U.S. State Department.
- Leave behind any government identification (badges, security passes, phone numbers, etc.) which are not necessary for the trip.
- Ensure that you have all official documents, i.e., passport, shot records, official orders, international driver’s license, etc.
- Grant power of attorney to an immediate relative/close friend. Complete or update your will to include naming a guardian for any minor children.
- Establish a point of contact for your family to call in an emergency.
- Carry an extra set of eyeglasses and any necessary medications, along with a copy of the prescription and the generic name of the drug, in your carry-on luggage. Keep all medications in their original containers.

DURING YOUR STAY

CARRY IDENTIFICATION

- Make copies of your airline ticket, passport Identification page, driver’s license and the credit cards you take with you. Carry this record in a separate place from the originals. This will help speed the replacement process if these documents are lost or stolen.
- Take all essential personal and medical identification to get you successfully through your trip.
- Do not leave your wallet or purse unattended.
- Do not take unnecessary credit cards and identification. This will minimize your replacement efforts and risks.
PASSPORT PROTECTION

- Your passport is the most significant identification you will carry. This is your proof of U.S. citizenship while traveling abroad. Travelers should be warned that passport theft, particularly of American tourist passports, is on the increase. You should treat your passport with the utmost care and protect it as you would your wallet. Take extra precautions to protect your passport as its loss or theft may cause you unnecessary travel complications as well as significant expense.

- To minimize potential loss or theft, it is recommended that you carry your passport in a front pants pocket or in a pouch hidden in your clothes. The only time your passport should leave your possession is if your hotel requires you to leave it at the desk during your stay. Some areas use this procedure to register you with the local police—a routine policy. Don’t forget to ask for a receipt and be very sure to retrieve your passport before continuing your trip.

- Use discretion in displaying this document, as it could draw undue attention to you. Memorizing your passport number and other essential information will help you avoid flashing your passport around when filling out items such as landing cards and hotel registration forms. If your passport is lost or stolen abroad, report the situation IMMEDIATELY to the nearest U.S. Embassy or Consulate and to the local police authorities. Again, having copies of your passport identification page and/or birth certificate will help speed the replacement process.

ESTABLISH POINTS OF CONTACT

- Establishing a point of contact is important. Someone should know your whereabouts from the time you depart the U.S. until you return home. Provide your contact with a detailed copy of your itinerary and advise him/her of any changes.

- If you are traveling on business, you should establish a point of contact in the country you are visiting. Be sure to carry that person’s name and phone number with you.

- Depending on your personal circumstances or if your travel involves an extended stay, it may be advisable to register with the nearest U.S. Embassy or Consulate. This will make it easier should someone at home need to locate you urgently or in the unlikely event that you need to be evacuated due to an emergency.

KEEP A LOW PROFILE

- You need to use common sense and be extra conscious of your appearance and actions so that you don’t attract unwanted attention. Take a good look at the items you plan to take with you such as clothing, jewelry and even religious items. This is especially true for reading materials that may be considered offensive. Keep in mind that certain items may not be appropriate for other areas.

- Avoid clothing and other outward vestiges that unnecessarily advertise you are an American citizen. Wear nondescript, casual apparel that enables you to blend in as well as possible. Leave behind the NFL sweatshirts, major league baseball caps and western apparel.

- Members of the armed forces should avoid wearing their military uniform unless required to do so.
SHUN PUBLICITY

- Shun publicity and inquiries by the local news media. If approached by the media, remember not to disclose any information relating to yourself or other government personnel and to report such contacts.
- Discussing personal and background information concerning family members with foreigners should also be avoided.

AVOID CIVIL DISTURBANCES

- Every effort should be made to avoid civil disturbances and disputes with local citizens.
- Use caution if you come upon a demonstration or a rally. If the speaker is denouncing U.S. policy, the crowd could become hostile to any American bystanders. Should violence break out, arrests are sometimes made indiscriminately. In the confusion you could be arrested or detained even though you are only an “innocent bystander”.

LOCAL LAWS

- Remember that although you are an American citizen, you are subject to the laws of the country in which you are traveling. Do not assume that what is acceptable in the United States is acceptable abroad. For example, in many countries, individuals are prohibited from making derogatory comments about the government or government leaders.
- Taking photographs of government facilities and religious symbols is also prohibited in many countries. Therefore, be aware of the local laws and as a general rule, do not attempt to take photographs in the vicinity of foreign military bases or buildings.

MONEY MATTERS

- Take most of your money in international traveler’s checks. Do not carry large amounts of cash.
- Plan ahead to ensure that you will have enough foreign currency for the expenses you anticipate during your first day in country. It is advisable to exchange some money to cover such essentials as taxi fares, meals, tips, etc. Keep small bills. Some countries have serious counterfeiting problems and large bills may be exchanged with counterfeit change.
- Do not count on currency exchanges at foreign airports being open 24 hours a day. Local banks usually offer the best rates, although hotel money exchanges may be more convenient.
- Always deal with reputable, established currency exchanges; in many countries it is illegal to do otherwise. If you deal with people on the street who offer you an “unbelievable deal”, you run the risk of getting counterfeit currency or being arrested for involvement in black market activity.
- Be sure to keep track of all your transactions. Each time you cash a traveler’s check record the serial number, denomination, date and location of purchase. Keep this in a separate place so replacement checks can be issued quickly if they are lost or stolen.
- Safeguard all credit cards as well as customer copies of each credit card transaction you make.
- Any credit cards which are unnecessary or invalid overseas (e.g., gasoline credit cards) should be left behind.
AIRPORT SAFETY

- Once you have landed, proceed directly to the baggage claim and customs areas. Keep a low profile and when processing through customs be courteous and cooperative.
- Stay alert, check out emergency exits and keep your distance from unattended luggage.
- Do not leave your own belongings unattended.
- Never, as a favor or otherwise, agree to carry a package for a stranger.
- Exit the airport as quickly as possible.

PERSONAL SAFETY

- Always be conscious of your surroundings and avoid any areas you believe may put your personal safety at risk.
- Be especially careful not to flash large sums of money. It is also best to leave your valuables (anything of high monetary or sentimental value that you can’t afford to lose or will be unable to replace) such as jewelry or expensive luggage at home.
- Avoid known high crime areas and never travel alone after dark.
- When traveling on foot, walk only on well-lighted, heavily-traveled streets whenever possible.
- Avoid shortcuts through alleys or side streets. Walk in the middle of the sidewalk and secure your belongings.
- Be wary of street vendors and innocent-looking youngsters. It has been reported that while one person has your attention, someone else may be picking your pocket.
- Should you be approached by a suspicious looking person on foot, cross the street or change direction. If you are threatened by the occupants of a car, move in the direction opposite to that in which the car is traveling.
- Learn a few phrases in the local language so you can obtain assistance if needed. You should also learn how to use the public telephone and carry the coins necessary to do so.
- Remain alert and if you have a problem go to the local police department.
- Avoid traveling alone.

HOTEL SAFETY

- Avoid taking a street level room. Choose a room between the second and eighth floors, i.e., too high for easy outside access and low enough to be reached by fire equipment.
- Use elevators rather than stairwells. Stand near the control panel so if threatened, you can push the alarm button.
- Locate exits within the hotel and develop a plan in case of fire or other emergency.
- Report lost keys immediately and consider changing rooms.
- When in the hotel room, secure the door and windows and keep them locked. When you leave your room, don’t leave indicators showing that you are out. In fact, leave the television or radio on, giving the impression that the room is occupied. Don’t leave anything of value (money, tickets, camera, etc.) in your room when you go out, even if it is locked in your suitcase.
- Do not accept deliveries to your room unless previously arranged and you are certain of the source and contents.
- Keep your room key with you instead of leaving it at the front desk.
• In some countries, you may be required to leave your passport at the hotel reception desk overnight so local police officials can check it. These are normal procedures required by local laws. Be sure to obtain a receipt for your passport and any valuables you leave in the hotel safe.

**DRIVING OVERSEAS**

• Check with the Automobile Association of America (AAA) if you plan to drive while overseas to determine whether you will need an international driver’s license. While some countries do not recognize U.S. driver’s licenses, most do accept international driver’s licenses and the latter are often required by foreign car rental agencies.
• Check with your insurance company before you leave to make certain you’re covered for driving while overseas. In some instances, supplemental insurance may be needed.
• Drive carefully while you are abroad! Many countries deal harshly with foreigners who are involved in traffic accidents. Drivers are often detained in jail while such accidents are investigated.
• Take care not to speed as some countries impose a speeding fine which is payable when levied.
• In some areas it is unlawful to use insulting language toward another person or to use abusive gestures while driving.

**VEHICLE SAFETY**

• Avoid selecting cars that mark you as an “important foreigner.” Rental cars are easy to spot so do not choose a large, flashy vehicle.
• Make sure the car is in good repair and always keep your gas tank at least half-full.
• Always drive with the doors locked and the windows up.
• Be cautious of anything that causes you to make an abnormal stop.
• Never pick up hitchhikers and if you come across an accident, drive to the nearest telephone or police station to report it.
• Always lock your car when unattended and avoid leaving valuables in the car even if locked in the glove box or trunk.
• Inspect your vehicle for tampering inside and out. If you suspect a problem, keep clear of the vehicle and contact the authorities.

**DEALING WITH PROBLEMS**

**ILLNESS OR MEDICAL EMERGENCY**

• Carry a summary of your medical history, to include past illnesses, allergies, and blood type.
• Carry an ample supply of any prescription medication you are required to take. It is also recommended that you take along an extra prescription in case you need a refill. Be sure to ask for the generic name of any prescription drug as brand names differ in other countries.
• Always leave medicines in the original labeled containers.
• Check with your medical insurance agent to make sure your medical expenses will be covered if you incur an injury or illness while traveling abroad.
• To help prevent illness while you are abroad, get a medical checkup before your trip and make sure that your immunizations are up-to-date.
• Do not hesitate to seek medical assistance if you need it. Should you require medical services due to injury or serious illness, contact the nearest U.S. Embassy or Consulate where a representative is on duty 24 hours a day. This individual can provide the names of reputable physicians and hospitals which can help you avoid improper treatment and/or large medical bills. In most cases, hotel personnel also provide good advice, although there are clerks who have arrangements with unethical physicians.

ARRESTS
• If you are arrested for any reason, ask permission to notify the nearest U.S. Embassy or Consulate.
• In some countries your request may not be honored immediately. Be persistent.
• A consular officer cannot arrange for free legal aid or provide bail money for you. He/she can provide you with names of English-speaking attorneys and help you find adequate legal representation.
• He/she can also contact your traveling companions or relatives in the U.S., or intervene if you are receiving discriminatory treatment.

OTHER UNFORESEEN CIRCUMSTANCES/SITUATIONS

During your travels, it will be most unlikely that you will ever be hijacked, kidnapped, held captive, or become a victim of terrorists or criminals. You should be aware, however, that the terrorist and criminal threat varies from country to country and that sometimes dangerous or unforeseen circumstances may occur. The information provided in the following sections is not meant to alarm you but is simply provided as guidance.

EVADING TERRORISTS AND CRIMINALS
• Get as much information as you can about the threat in your destination before you leave, especially if traveling to a high-risk area.
• It is strongly recommended that you contact the State Department for additional information prior to traveling. Recorded messages provide information and travel advisories, if warranted, for most regions of the world.
• Develop and implement a security plan upon your arrival.
• Do not become complacent in low risk areas. Situations sometimes change rapidly. In general, terrorists and criminals alike strike when and where they sense their targets to be most vulnerable and they are most successful when security measures are lax and daily routines are predictable.
• Vary arrival times, departure times, and routes which you normally take.
• Be alert to the possibility of surveillance. If you believe that you are being followed, do not challenge your follower; instead, attempt to mentally note his/her physical characteristics, type of car, license number, etc.
• Promptly report such incidents to security officials at the site where your security officer and/or at the nearest U.S. Embassy or Consulate.
HIJACKING/HOSTAGE SITUATION

- Try to remain calm and alert and avoid doing anything that might attract undue attention to yourself.
- Comply with orders and instructions without complaining. Keep in mind that what you say and do could impact others.
- Be as general as possible if questioned and do not discuss anything which you are obligated to protect.
- Be non-threatening in conversations with your captors and avoid arguments and physical violence.
- Prepare yourself for experiencing depression, boredom, and frustration since a hostage situation may continue for an indefinite period.
- Try to humanize the event as much as possible. If you need anything ask for it, making your request in a reasonable low-key manner.
- Try to establish a program of mental and physical activity if your situation becomes lengthy and drawn out.
- Above all, rely on your inner resources and think positively.

A REMINDER
Remember that our country will be judged by the impression you make. As an American abroad, you serve as a spokesperson for the United States. Don’t be surprised if you occasionally encounter anti-American sentiments in some foreign countries which you visit. If you wish to avoid political discussions, state that you are not well versed on all phases of American domestic and foreign policies then change the subject. Do not get involved in comparing other countries unfavorably with the United States. From time to time, all travelers experience frustrations such as crowded hotels, unavailable rental cars, overbooked restaurants, and delayed plane flights. Common sense and good judgment should govern your reactions in such situations. Stay calm and don’t be overly critical of local customs or conditions which you find disagreeable.

UPON YOUR RETURN
Be sure to report any unusual circumstances or noteworthy incidents to your Security Officer and/or the FBI upon your return. Your Security Officer ensures that other travelers from your organization are aware of the general security precautions, as well additional threats you report. Notifying the FBI will help to ensure the FBI travel briefs and the official U.S. Department of State Travel Advisories take into consideration any unusual circumstances or noteworthy incidents you encountered during your travel.

HAVE A SAFE AND ENJOYABLE TRIP
Now that you are aware of the basic precautions that should be taken during your trip, take some time to put all this information into perspective. If you follow these precautions, you will reduce the risk of encountering problems. Also, the more you learn about passports, visas, customs, immunizations and other travel basics will help you prevent problems before they occur. Additional information may be obtained by contacting the agencies listed below. It may be helpful to carry these numbers with you.
DEPARTMENT OF STATE CITIZENS EMERGENCY CENTER
ASSISTANCE TO TRAVELERS
(Current travel advisories)
(202)647-5225

INTERNATIONAL ASSOCIATION FOR MEDICAL
ASSISTANCE TO TRAVELERS
(List of English-speaking doctors practicing in foreign countries)
(716)754-4883

U.S. CUSTOMS 24-HOUR EMERGENCY
Toll Free Number
(800)522-5220

TRAVEL ADVISORIES
There are three types of State Department travel advisories:

- WARNING - recommends deferral of travel to all or part of a country.
- CAUTION - advises about unusual security conditions, including the potential for unexpected detention, unstable political conditions or serious health problems. (Not intended to deter travel to a country)
- NOTICE - provides information on situations that do not present a broad-scale risk, but which could result in inconvenience or difficulty for traveling Americans.

To obtain travel information (Travel Advisories) or a specific country or geographic region, contact the U.S. Department of State by Phone or mail. You can also obtain current Travel Advisories at the U.S. Department of State.

United States Department of State
Bureau of Consular Affairs
Washington, D. C. 20520
(202)647-5225
http://travel.state.gov