

APPENDIX 5 TO ENCLOSURE 2

DEFENSIVE SECURITY BRIEFING

1. INTRODUCTION. Persons granted access to SCI incur special security obligations and should be aware of possible risks inherent to foreign travel. Persons planning foreign travel should contact their SSO to determine their organization's foreign travel and foreign contact policy. The following information is a general purpose travel briefing. Detailed briefings may be obtained from the nearest military intelligence or counterintelligence representative.

2. PURPOSE. U.S. military, Government, civilian and defense contractor personnel are considered prime targets of Foreign Intelligence Services and terrorist groups. The purpose of this briefing is to acquaint the traveler with the risks involved in traveling to foreign countries and to furnish you guidance that may enable you to minimize those risks.

3. BACKGROUND. Many foreign countries offer interesting travel brochures, special rates, and other inducements through U.S. branches of their travel bureaus in efforts to attract the growing number of Americans traveling abroad. Past cases reveal that American personnel performing such travel may be subject to surveillance and collection operations by the various foreign intelligence services. Travelers may also be subject to terrorism or other acts of violence either by design or by circumstance.

4. FOREIGN INTELLIGENCE SERVICES (FIS)

a. All foreign countries actively engage in the collection of intelligence information. However, whether they are "hostile," "neutral," or "allied," there is no such thing as a "friendly" foreign intelligence service.

b. The main objective of any FIS is to gain advantage for their nation through the collection of information. Currently, the most prized type of intelligence is scientific and technological data, followed by the classified Government information, but unclassified material--even material which appears to be trivial can also be of inestimable value. Potentially, the most valuable sources of information are those acquired through the use of individuals recruited as agents by FIS. In addition to penetrating the Government and its official organizations, the penetration of commercial businesses, educational and private institutions involved in sensitive, national defense-related research and development work can be of tremendous value. Of course, the single greatest achievement an intelligence organization can have is the placement or recruitment of an agent directly in a sensitive position in a national defense or intelligence element of another government.

(1) FIS are relentless and seek information wherever, whenever, and from whomever they can and employ any and all tactics necessary to target, recruit and exploit potential sources. Among the tactics they may use against U.S. personnel is a smooth, subtle, seemingly guileless

approach—befriending targets, treating them to gifts or money, wining and dining them in the belief that Americans are hopeless materialists who can be swayed easily by appeals to their greed.

(2) Recognizing that most Americans are generally friendly and gregarious people who enjoy talking to others, FIS operatives frequently employ a seemingly innocuous and very effective method of intelligence gathering known as “elicitation.” Elicitation is the art and science of engaging someone in simple, “innocent” conversation for the purpose of getting the targeted individual to speak openly and more in-depth and, possibly reveal classified information on topics of interest to FIS operatives. Practiced by experts, the target of elicitation may not even realize that he or she has been elicited until “too much” has been said. Elicitation is smooth and insidious. Beware of it!

(3) In another maneuver known as the “False Flag” approach, an FIS operative misrepresents himself as a citizen of a country friendly to the United States. Thus, a targeted American may be duped into handing over information by being led to believe he is aiding an ally of the United States. In a variation of this tactic, FIS agents may pose as representatives of a country towards which a targeted American is particularly sympathetic. Also, if an FIS agent believes an individual has similar sympathies, he or she may make an appeal for information based on ideology. A “pitch” for information may also be geared to take advantage of an American’s desire for international harmony and world peace. Similarly, certain FIS organizations not only routinely charge their own citizen-students studying abroad in the U.S. to collect information but, also regularly target Americans of their own ethnicity using a variety of tactics to include everything from bribery and patriotic appeals to support their “mother country” to outright blackmail and threats.

(4) Another favored appeal exploits the American belief in freedom of speech and the free exchange of information. For example, an FIS agent in the role of a scientist may suggest to an American scientist that science has no political boundaries. Therefore, in the interest of science, the American is encouraged to share his knowledge with a fellow “member” of the international scientific community.

(5) FIS also use aggressive means in their ceaseless quest for strategic information. Espionage is their business and patriotic duty. If they feel coercion and blackmail shall serve their purpose, they shall not hesitate to employ those methods. As you travel, do not place yourself in a compromising position by engaging in abnormal or promiscuous sexual behavior, black marketing, violating local laws, or photographing or straying into restricted areas. FIS keep travelers under constant surveillance by using agents, video and photographic surveillance, and bugging devices in hotel rooms, bars, restaurants, lounges, and telephones. Such methods may provide them the material to entrap an unwary traveler.

(6) Harassment and provocation are other tools that may be employed by FIS. Travelers may be placed in unusual situations that may cause an incident or elicit a response that would entangle or compromise an individual.

5. TERRORIST, CRIMINAL, AND MOB VIOLENCE

a. Terrorists have a different objective than FIS—they are interested in “sensationalism” or other use that can be derived from the compromise, embarrassment, interrogation, kidnapping, or death of a U.S. citizen. The threat changes constantly and is contingent upon the country and area visited along with world events. However, from a general perspective, the threat of terrorism to a traveler should be considered minimal, unless the traveler happens to be in the wrong place at the wrong time. As with FIS, a terrorist group must know the “who, where, when, and how,” to target a specific individual. Therefore, maintaining a “low profile” and not drawing undue attention to one’s affiliation with the U.S. Government is essential. Even though an individual may not be targeted for terrorism, an individual can still become a victim of terrorism. Being in the wrong place at the wrong time may be unavoidable, but the risk of being a chance victim of terrorism can still be reduced. Remember, most terrorists select “soft” targets like commercial establishments and individuals residing within that country. For the most part, except in situations where FIS is supporting, sponsoring, or otherwise has a relationship with a particular terrorist organization, terrorists do not have sophisticated collection capabilities to determine names of a traveler and then target that person. They prefer to concentrate on individuals residing in-country.

b. Criminal or Mob Violence. No matter where anyone travels, criminal elements (thieves, muggers, etc.) are present. The foreign traveler is a good target because the traveler may be disadvantaged by being in an unfamiliar place, ignorant of local laws, and unable to freely communicate because of a language barrier. In unstable political areas or where the United States is unwelcome, the presence of a U.S. citizen may be enough provocation to cause an incident or become a victim of mob violence. Any minor incident or breach of law or custom involving a U.S. citizen can be blown vastly out of proportion creating a much larger incident.

6. TRAVEL GUIDANCE. Common-sense rules for any traveler are often overlooked in the rush to acquire tickets, hotel reservations, visas, etc.:

a. Personal Concerns

(1) Travelers should not reference their intelligence affiliation or access to classified information.

(2) Travelers should not bring any personal objects with them that they cannot afford to lose. This applies especially to jewelry items. Carry traveler’s checks and one or two major credit cards, not large amounts of cash.

(3) Travelers should make a copy of the identification page of their passport before their departure and take it with them. Copies should be kept separate from the passport itself. Also, travelers should memorize their passport number. While traveling, travelers should leave their passport and any unneeded money locked in a hotel safe-deposit box. If local law does not require persons to keep their passport with them, travelers should carry only the photocopy of their passport and driver’s license when leaving the hotel.

(4) Travelers should advise the U.S. Embassy in each host country of their complete itinerary. Keep in contact and record the address and telephone number of the U.S. Embassy or Consulate in each host or major city in which a visit is planned.

(5) Travel with several passport size photos. In some areas, it can be difficult to replace photos on short notice if your passport is lost or stolen.

(6) U. S. driver's licenses are valid in Canada and Western Europe; elsewhere you shall need an international driver's permit available from the American Automobile Association. Even with an international permit, foreigners are forbidden to drive in countries such as Egypt, Vietnam, China, and Nepal. Know local traffic laws and penalties, which may be severe. In Indonesia, for example, fines for not wearing a seat belt can be \$1,500.

(7) The Department of State, Bureau of Consular Affairs, Office of Overseas Citizen Services provides current, country-specific threat information and offers consular information sheets, travel warnings, public announcements, tips for travelers brochures, visa bulletins, and other consular information. Callers outside the Washington, D.C. metropolitan area are charged the cost of a long distance phone call, but there are no additional charges for this service. They may also be contacted through the internet at www.travel.state.gov.

(8) Information on vaccinations and other health precautions, such as safe food and water precautions and insect bite protection, may be obtained from the Centers for Disease Control and Prevention's (CDC) hotline for international travelers at 1-877-FYI-TRIP (1-877-394-8747) or via www.cdc.gov/travel for reports of medical alerts in foreign countries.

(9) Travelers should ensure their medical insurance covers the travel. Personal health insurance policies may be valid while you are visiting Europe, but may not cover individuals while white-water rafting in Canada.

(10) Carry ample supplies of pain relievers, antacids, diarrhea and motion-sickness remedies, antibiotic cream, gauze bandages, water-purification tablets, insect repellent, sunscreen and prescription medication.

(11) Travelers should carry prescription medications in their original containers. Travelers can be detained during a custom's search and questioned concerning the pills.

(12) Medical or dental service should be obtained only from a U.S. Government facility or from persons or institutions approved by U.S. Embassy officials.

b. Hotel Concerns

(1) Be careful about leaving items in hotel room safes. Safe-deposit boxes in a hotel lobby are better, but the best are similar to those in a U.S. bank, with two keys and under 24-hour observation. Do not leave valuables or important papers lying around your hotel room.

(2) Do not stay above the sixth floor. Many foreign fire companies do not have ladders that go beyond this floor. The third floor is your best choice. Occupants of rooms lower than the third floor are subject to a higher degree of burglaries or robberies by people entering from the street.

c. Airport and Customs Concerns

(1) Be careful to make an accurate and complete declaration of money (including traveler's checks), credit cards, and all valuables (including cameras and jewelry whether worn or carried). It is imperative to retain a copy of this declaration until departure. Use only authorized banks and currency exchanges.

(2) Security screening process at international airports shall vary depending upon the country visited. Arrive at the airport at least 2 hours prior to departure. This allows for ample time to pass through the security screening process. Do not linger in the airport ticketing area after checking-in. This is the most vulnerable section of the airport and has been the repeated target for terrorist groups. Proceed to the security area as soon as possible. Questions asked by airport security officials may sound like the officer is conducting an interrogation. The officer is looking for indications of possible criminal or terrorist activity. Be cooperative and answer all questions truthfully. Airport security officials may be especially concerned with electronic devices, so travelers should be forthcoming about any in their possession. In Germany, airport officials have been known to request individuals to extract the batteries from the devices before boarding the aircraft. Other countries may have similar policies.

(3) Laptop computers are a focus of security people because they have been used to hide drugs and explosives in the past. Countries in Central and South America and Europe may be particularly concerned with laptop computers. Persons traveling with a laptop should be prepared to demonstrate its functions at all security checkpoints.

d. Crime Prevention

(1) Contact a DAO or Consulate or Embassy Regional Security Officer about the local situation if necessary. Find out which parts of town local inhabitants consider risky. Stay in well lit areas; do not use short cuts or narrow alleys. Be especially alert in crowds. Thieves often strike when travelers are distracted. The most common sites for thefts to occur are tourist spots, shopping areas, transportation centers, and train stations. Dress modestly and be discreet.

(2) Theft is common on overnight trains. Place luggage under the seat rather than on overhead racks. Keep valuables under the pillow or in a safe pack around the neck or waist. If traveling in a group, sleep in shifts.

(3) Men, if possible, should keep their wallet in a front pocket. Frustrate pickpockets by taking the following precautions: wrap rubber bands around the wallet to make it difficult for a pickpocket to remove it, keep the wallet with a comb through the fold with the teeth facing upward so it shall catch on the pocket lining if removed, place a handkerchief over your wallet or place the wallet in your pocket sideways. Women, if possible, don't carry a handbag. They are considered

an “easy target” for thieves. They simply take the bag and run, resulting sometimes in physical injury to the carrier. If travelers need to carry a handbag, do not carry money or identification in it. Hide all valuables on your person. Money belts or pouches worn on the outside of clothing or loosely hung around the neck are easily cut or ripped off. Remember, wearing them on the outside highlights where you keep all your valuables.

(4) In areas noted for carjacking or tourist robberies, make sure rental vehicles do not have special license plates or agency stickers.

(5) When driving, stow belongings in the car’s trunk rather than on the back seat. Keep windows up and doors locked. Empty the trunk at night, even if the parking area is guarded.

(6) In the event of a flat tire, drive to a service station or busy intersection before stopping. If the vehicle breaks down, wait inside for assistance from police or an authorized repair person with proper identification.

(7) Be cautious of sexual overtures from anyone. Aside from the potential health hazards, prostitutes are often the decoys who steer you into becoming a victim of other crimes, such as robbery and extortion. From a CI perspective, offers of sexual companionship have historically been a method used by FIS in an attempt to compromise Government employees and Government contractors.

(8) Attempt to know the laws and rules of the country to be visited. Do not engage in black marketing or other illegal activities. Do not engage in black market currency exchanges or other illegal transactions. Depending upon the country’s exchange rate, the financial advantage of engaging in such activity may be substantial, but it is not worth the risk.

(9) Do not attempt to propagandize or engage in political arguments. Many foreign nationals are curious about the United States, and are genuinely interested in talking to Americans. Their questions are best answered in an objective forthright manner without drawing unfavorable comparisons with the country visited.

(10) Be careful about accepting invitations. Do not overindulge in drinking or engage in promiscuous activities. Audio (listening) devices and hidden photographic cameras are often planted in rooms. Depending upon the country visited, if invited to a foreign national’s residence, or to any other form of private gathering, try to keep at least one other member of your group with you. Travelers should maintain a healthy skepticism toward persons who seem to attach themselves to them. Overly friendly tourist guides, interpreters, or maids, who show an undue interest should put the traveler on the alert. Do not trust interpreters with matters of confidence.

(11) Do not accept letters, personal messages, photographs, packages, or other material to be carried openly or smuggled in or out of the country.

(12) Travelers generally are NOT under individual surveillance during visits; however, if he or she suspects that they are being watched, resist any temptation to “play games” with what may seem to be clumsy attempts to keep an eye on you. Do not attempt to lose real or imagined

surveillance by taking evasive maneuvers, searching your room for listening devices (“bugs”), or attempting to play tricks on such “bugs.” This sort of action only serves to arouse suspicion and may result in increased foreign security attention and possibly harassment.

e. General Comments

- (1) Do behave in a natural manner, use good judgment, and enjoy the trip.
- (2) Maintain a “low profile” by:
 - (a) Blending in with local populace.
 - (b) Wearing suitable attire -- do not over or under dress.
 - (c) Being sensitive to local customs and laws.
 - (d) Traveling in pairs or small groups of no more than four people.
 - (e) Using rental rather than official cars if possible.
 - (f) Not flaunting American citizenship or attaching an “air of importance” to yourself.
 - (g) Not being aggressive or insulting to the native population.
 - (h) Ensuring that your itinerary is not publicized, but given to those who have a “need to know.”
- (3) The following are suggestions for personal safety:
 - (a) Unobtrusively inspect under seats and seat cushions on airplanes or other modes of transportation.
 - (b) Inspect the rental vehicle for signs of tampering.
 - (c) Park and lock car in a secure area.
 - (d) Avoid lingering in potential threat areas such as general terminal areas at airports or lingering in front of official buildings being visited.
- (4) Never pick up souvenirs, statues, or artifacts just because they appear to be lying around or unclaimed. Purchase such items in approved shops only, making certain that a receipt is provided for each purchase. Do not sign any receipts for money or services, unless first assured of and furnished an on-the-spot copy which clearly identifies and itemizes the nature of the transaction.

(5) Do not make or write any statements that might be exploited for propaganda purposes. Do not sign petitions, however innocent they may appear.

(6) Do not photograph any military personnel, equipment, installation, defense plant, or other military or restricted area. Also, refrain from photographing slum areas, ghettos, or underprivileged persons in the host country. Do not photograph airports and train yards or other facilities that could be used for military purposes.

(7) As a precaution, be aware that clothing may be tagged with invisible dyes or radioactive materials. This can be done at a dry cleaning establishment or in your room. If a letter were placed in the tagged pocket and later mailed, it could be retrieved and traced.

(8) In writing letters, use personal stationery and not that given to you by any local hotel. Also purchase stamps at a post office or embassy. Stamps obtained at a hotel or other source can be tagged with invisible inks or radioactive tracers. Assume that letters shall be opened and read. If necessary to write about confidential matters, use appropriate channels of the Embassy or Consulate.

(9) If detained, remember, tourists generally have nothing to worry about so long as they follow the local rules, and use good judgment. However, occasionally individuals do encounter trouble with authorities; either by mistake, or as the result of some injudicious action. Should this occur, the most important things to remember are:

(a) Insist on being put in contact with the American Consulate at once. If the authorities stall or attempt to intimidate, refuse to make any statement until this has been done. Experience shows that if an individual cannot be intimidated by vague or implied threats, the detainer shall usually back down if the individual has not, in fact, done anything wrong.

(b) Under no circumstances sign any document until you have had the opportunity to meet with a U.S. official.

(c) Remain calm, but assertive. Do not antagonize Government officials, but continue to insist on your right to speak with a representative of the U.S. Government.

f. Hostage Situations. In the event of a hostage situation:

(1) Do not physically resist, but passively cooperate with captors.

(2) Prepare mentally for a long period of hostage negotiations.

(3) Remember that although negotiations are usually lengthy, virtually all hostages are released unharmed.

(4) Attempt to establish personal rapport with your captors, while at the same time maintaining personal dignity.

(5) Do not become involved in controversial discussions with the terrorists.

(6) When a rescue party approaches, lie on the floor with your hands covering your head; do not move until instructed to do so by members of the rescue team.

g. Air Travel. Military air or military/Government charter flights are preferred within CONUS. Non-stop commercial transcontinental flights are considered more vulnerable to possible hijacking than those making intermediate stops. Outside CONUS, every effort should be made to fly via military aircraft, diplomatic courier flight or military/Government charter flight. Commercial air travel aboard U.S. flag aircraft that does not have intermediate, weather, alternate or landing rights in “threat areas,” or areas of high vulnerability to hijacking is recommended.

h. Hijackings. If U.S. military or Government civilian personnel should happen to be aboard an aircraft that has been hijacked:

(1) If in uniform:

(a) Be as unobtrusive as possible.

(b) Do not attempt to take charge, demand privileges of rank, or openly advise other passengers as to their conduct.

(c) If asked for identification, show only passport (tourist if possible).

(2) If in civilian clothing, do not offer to make known a U.S. military or Government affiliation unless forced to do so. Most persons previously placed in such a situation have been requested only to show some reasonable identification (e.g., driver’s license, passport, credit cards).

(3) The traveler must keep in mind that, these are only “guidelines,” not “hard and fast” regulations that apply in all situations. The world and the rules have changed since 9/11. There are no guarantees. In all situations be adaptive and flexible.

7. REPORTING PROCEDURES. If you suspect an approach has been made, or you become involved or entrapped in a conspiracy to commit espionage, you are to report to the nearest U.S. Consulate, Attaché, Embassy Regional Security Officer or Post Duty Officer. If you have been indiscreet or otherwise compromised, he or she shall discuss the situation in confidence with a U.S. security representative. Above all, do not attempt to get out of an embarrassing situation by yourself, or assume the role of a self-appointed counterintelligence agent.

8. ADDITIONAL INFORMATION. Any suspected approach made subsequent to travel should be reported through the traveler’s security officer or commander to the appropriate counterintelligence organization.