DEFENSIVE SECURITY & FOREIGN TRAVEL BRIEFING

It is increasingly apparent that foreign countries are targeting newly developed, critical technologies (usually unclassified) having direct military application. This includes dual-use technology such as integrated circuitry, fiber optics, and software that have both military and non-military uses. In the international market place, many of our competitors view industrial espionage as a legitimate practice and will exploit vulnerabilities when they see them.

TRAVEL

When taking a business trip following the guidelines below will go a long way in helping ensure that you have a safe and uneventful trip.

1. Restrict trip and itinerary information to close family members and necessary business associates.
2. Use reliable hotels recommended by colleagues, the U. S. Embassy or Consultants.
3. Maintain a low profile. Avoid a display of company affiliation when registering at the hotel.
4. Ensure that locks on hotel room doors are in working order, utilize hotel vault or secure storage for valuables.
5. Do not leave identifying materials in the hotel room revealing who you are, why you are there, who you are to visit and when, or your schedule and return flight plans.
6. Avoid carrying large amounts of cash. Use traveler's checks.
7. Beware of friendly strangers, particularly if chance conversation reveals they are interested in your occupation
8. Avoid actions identifying you as an American or someone wealthy or important.
9. Avoid establishing routine schedules.

When travelling by automobile:

1. Keep your vehicle in good running condition, keep the gas tank at least half full at all times.
2. Be alert to your immediate surroundings at all times.
3. While driving, keep car doors locked and windows open no more than two inches.
4. Use well-traveled highways, remain alert at all signals, stop signs and intersections when slowing down or stopping.
5. Be suspicious of distress signals, such as auto breakdown with motorist asking for assistance.
6. Do not pick up strangers.
7. Lock unattended cars, no matter how short the duration.
8. Separate ignition key from other keys if leaving key with parking attendant, park off the street at night, preferably in a locked garage or attended lot.
9. Avoid using cabs for sightseeing, take bus tours instead.

Travel on commercial airlines has become one of the most secure means of travel in the United States. Ground security measures and other anti-terrorism techniques have made the threat of risk when flying commercially far less than when traveling by other means.

However, keep in mind that in most overseas locations, ground security measures may not be as effective as those in this country. Remember the following items:

1. Fly U.S. carriers whenever possible.
2. When overseas, do not make reservation changes by phone.
3. Leave early for the airport to minimize exposure.
4. Once in the terminal, move as quickly as possible to secured areas, past screening points, and stay there.

The chance of your being taken hostage is highly unlikely, unfortunately, it does happen. If you are in an aircraft, boat, train or terrorists have captured building that and you are being held as part of a group of hostages, your ability to act appropriately will be very important for personal safety and may greatly enhance your chance of survival. If you become engaged in a hostage incident, remember the following:

1. Try to remain calm.
2. Obey the terrorist orders.
3. Be courteous and polite to the terrorists and other hostages, do not debate, argue or discuss political issues with the other hostages or terrorists.
4. Talk in a normal tone; avoid whispering and making abrupt movements.
5. Locate yourself away from windows and doors and as far away from the terrorists as possible.
6. Answer questions immediately unless your position or purpose of travel may pose a threat to terrorists or to their ideologies.
7. Inform your captors if you have any medical condition or special disabilities.
8. Do not discuss possible actions that may be taken to your family, friends or company.

FOREIGN INTELLIGENCE

The main objective of foreign intelligence is the collection of data. Operatives in this field employ various tactics in their campaigns to target employees. Operatives may befriend targets of their own ethnic group, recruit foreign employees within a U.S. firm to steal proprietary or classified information, or task foreign students studying in the U.S. to acquire information on economic and technical subjects.

The operative of a Foreign Intelligence Service (FIS) need not be a foreigner, nor need the occasion of encountering him or her be in an extraordinary manner. The operative may be an individual you meet at a conference, symposium, or a fellow American who has been recruited as an agent by a FIS.

Events-such as conferences on high-tech topics, trade fairs, and air shows attract many foreign scientists and engineers, providing foreign intelligence collectors with a concentrated group of specialists on a certain topic. Collectors target these individuals while they are abroad to gather any information the scientists or engineers may possess. Depending on the foreign country and the specific circumstances, some elicitation efforts can be heavy-handed and threatening, while other times they are subtle.

It is important to remember that unclassified information, company proprietary material and technical data may be just as valuable to our adversaries as classified material.

SUSPICIOUS CONTACT

Employees who are authorized access to classified information are important targets for FIS. It is common practice for a FIS to establish and maintain dossiers on personnel of intelligence interest, particularly of personnel whose jobs afford them access to classified and unclassified information or technical data in any area of special interest. The FIS are constantly on the look out for opportunities to gain any kind of advantage that can be exploited.

Therefore it is required that you report any individual, regardless of nationality, that approaches you to obtain illegal or unauthorized access to classified, proprietary, and technical information.

DISCLOSURE OF INFORMATION TO NON-U.S. CITIZENS

Classified information may not under any circumstances be disclosed to representatives from a foreign country. Before any unclassified information or technical data associated with a classified contract may be disclosed, prior approval must be obtained by the appropriate owner of the information (i.e., NSA, DOE, DOJ, etc).

Unclassified technical data, pertaining to items on the 'Commodity Control List" may require approval by the Department of Commerce prior to release to a non-U.S. citizen or foreign country.

CONCLUSION

The U.S. can be weakened by the theft of its vital knowledge, and its enemies can be strengthened by the acquisition of that knowledge, whether it is classified or unclassified. It is the responsibility of each individual who has been entrusted with sensitive information to do his/her share in protecting America's critical technology and strategic knowledge.

I certify that I have received from Mr. William E. Brown, Fort Leavenworth Installation Anti-terrorism Officer, a Defensive Security & Foreign Travel Briefing. I fully understand my responsibility for safeguarding U.S. Government, company classified, proprietary and technical information and have directed any questions I have to my Security Representative.

Printed Name	SSN
Signature	Date