# DEFENSIVE TRAVEL BRIEFING

## PURPOSE

As an employee of a defense contractor, you have access to critical U.S. government information. The purpose of this briefing is to remind you of your responsibilities to protect the information, report specific incidents which may occur, and to remind you of some specific vulnerabilities associated with foreign travel.

The companies’ involvement in government contracts requires us to maintain security awareness programs, which include formal briefing of the threat posed by foreign intelligence services especially while employees travel to and around foreign countries.

This Defensive Travel Briefing is part of that program.

## THE NATIONAL SECURITY THREAT LIST

The FBI consider the following to be threat to our national security regardless of the country involved:

ANY foreign intelligence activity which is:

* Targeting U.S. intelligence and foreign affairs information and U.S. Government Officials.
* Directed at classified or critical technologies.
* Directed at the collection of U.S. industrial proprietary economic information.
* Directed at the collection of information relating to defense establishments and national preparedness.
* Involving the proliferation of special weapons of mass destruction.

If you become aware of or suspect any activity aimed at the above list, notify your security officer.

## PRIOR TO DEPARTURE

Contact your security officer to obtain the most recent travel advisory information. You should also want to review the Department of State travel advisories for the countries and region you expect to be in or near: <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/>.

Carefully complete your Visa application, as it will be scrutinized. If you are a naturalized U.S. citizen returning to the country of your origin, your citizenship may be questioned. If you encounter such a problem, please contact the State Department for guidance.

Contact the American Embassy or Consulate prior to your arrival and provide your local address and probable length of your visit. For most official business visits, a cable should be sent to the appropriate embassy advising of your visit. You are encouraged to enroll in the Department of State’s Smart Traveler Enrollment Program (STEP). <https://step.state.gov/step/>

Ensure that items you carry with you are not prohibited or controversial. Political material or anything that might be considered pornographic should not be carried. If you are carrying prescription drugs with you, be certain that they are clearly marked and bring only necessary quantities.

Carrying letters, packages or gifts to individuals in other countries should be avoided. You may be viewed as a courier attempting to bring the material for subversive or illegal purposes.

DO NOT TAKE CLASSIFIED MATERIAL or any sensitive information with you as you travel. If you will need sensitive material while traveling, arrange to have the material transmitted by other approved means prior to your departure. Consult with your security officer for guidance.

Limit the amount of identification that you take. If you have several forms of Government ID (i.e. Federal ID, building passes, courier cards), bring only one ID with you. Make a photocopy of an ID or credit card you will be bringing and leave the photocopy at home. Write down your passport number and keep it separate from your passport. Do the same with your address and telephone number.

The carrying of laptop computers is discouraged, but not prohibited. Consult your security officer and your Information Technology Security Officer if you plan to take a laptop.

## UPON ARRIVAL

An accurate declaration of all money and valuables should be made at entry. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money exchanges, as these frequently are required upon departure. Undeclared sums of U.S. or other currency are likely to cause difficulty with authorities and may be confiscated upon departure.

Declare such items as cameras, radios, etc., to preclude possible explanations, customs charges, or confiscation when you leave.

Use of public transportation is recommended rather than driving yourself, because involvement in traffic accidents can be problematic. Taxis are the preferred mode of transportation. State Department travel advisories proved updated information regarding public transportation concerns in the country you are visiting.

## YOUR ACTIVITIES AND BEHAVIOR

MAINTAIN A LOW PROFILE. Show discretion and common sense in all your activities. Refrain from any behavior that may make you conspicuous or a potential target. NEVER engage in any illegal activity, excessive drinking, or gambling. Use your best judgment to carefully avoid any situation which may allow a foreign intelligence agency the opportunity to coerce or blackmail you.

Do not discuss classified or sensitive information in any vehicle, restaurant, hotel room, hotel lobby, or other public place. In any public place, your conversation may be overheard, monitored, or recorded. If you need to call the U.S. to discuss classified or sensitive information, locate a secure telephone by contacting the Regional Security Officer at the U.S. Embassy.

If you locate any possible surveillance equipment, such as microphones, telephone taps, miniature recording devices, or cameras, do not try to neutralize or dismantle it. Assume the device is operable and that active monitoring is ongoing. Report what you have found to the U.S. Embassy or Consulate. When you return, advise your Facility Security Officer.

Never leave luggage or briefcases that contain sensitive information unattended. This includes leaving your briefcase in your hotel room. We encourage you to keep your briefcase or backpack, containing sensitive information, in your possession. Personnel often report their luggage or briefcase being searched or rummaged through. If this happens to you, report the incident to your Facility Security Officer when you return.

Foreign Intelligence Services may place you under physical surveillance or you may suspect that you are being watched. It is better to ignore the surveillance than to attempt to lose or evade it. In any event, your actions should be prudent and not likely to generate suspicion. Good precautionary measures are to use well-traveled highways and avoid establishing routine schedules.

Never try to photograph military personnel, military or government installations, or possibly "restricted areas." It is best to also refrain from photographing police installations, industrial structures, transportation facilities, government buildings, and border areas.

Beware of overly friendly or solicitous people that you meet. Do not establish personal or intimate relationships with these individuals as they may be employed by the intelligence service. Do not share any work-related information with any person who does not have a need to know.

Do not accept sealed packages and agree to transport them back to the U.S. Even if your friends, relatives, and professional contacts, make the request, do not accept the package.

If you will be on an extended visit and expect to be writing or receiving mail, remember that it may be subject to censorship. Never make references to any classified or sensitive information.

Avoid any areas where there is political or ethnic unrest, demonstrations, or protests.

Should you be detained or arrested for any reason by the police or other officials, be cooperative, and contact the U.S. Embassy or Consulate immediately. Do not make any statements or sign any documents you do not fully understand until you have conferred with an Embassy representative.

Do not leave documents in hotel safes.

You may keep this document for reference, but do not carry it with you.

## UPON YOUR RETURN

Contact your Facility Security Officer to accomplish an after-travel report. You may also be asked to provide details regarding any unusual occurrences or to report foreign contacts and any unusual incidents. You are required to report all contacts with individual of any nationality, either within or outside the scope of your official activities in which:

1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.
2. You are concerned that you may be the target of an actual or attempted exploitation by a foreign entity.

## EMERGENCY NOTIFICATION PHONE NUMBERS

Before your departure, it is recommended that you provide your family and/or a close friend with the name and phone number of your supervisor or coworker and the reverse, provide your family’s contact information to your supervisor so that you might be reached in the event of an emergency.

If and emergency does occur, persons needing to reach you should be instructed to contact who to contact. You may be able to also use the 24-hour State Department Operations Center (202) 647-1512, to assist in reaching you.

Tom Vaughan

Facility Security Officer

808-232-4004

tomvaughan@vaughansecurity.com