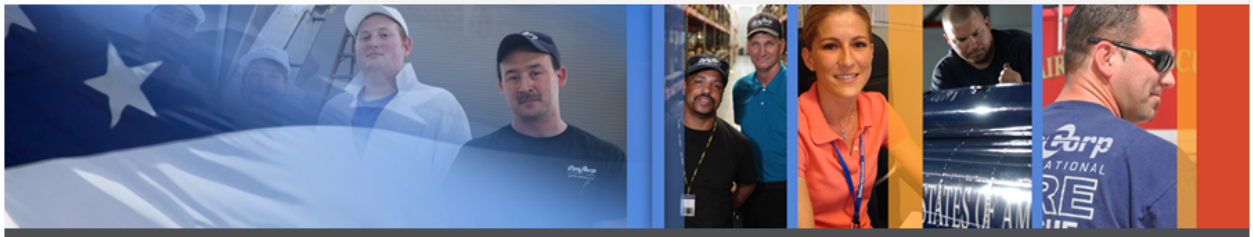
DynCorp International

The Responsibilities are Great



Foreign Travel Briefing

What you need to know

This briefing is applicable to all employees, subcontractors and consultants travelling internationally on behalf of DynCorp International LLC.

We Serve Today for a Better Tomorrow.™

Table of Contents

IMPORTANT RESOURCES FOR INFORMATION WHILE TRAVELING OVERSEAS

International travelers are encouraged to enroll in the free Smart Traveler Enrollment Program (STEP) offered by the U.S. Department of State.
https://step.state.gov/step/

Travel Tips
http://travel.state.gov/travel/tips/tips_1232.html

Travel Warnings:
http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html

Finding a hospital or doctor abroad:
http://travel.state.gov/travel/tips/emergencies/emergencies_1195.html

Victims of crime:
http://travel.state.gov/travel/tips/emergencies/victims_crime_overseas/victims_crime_overseas_1748.html

Emergencies: In the event of financial emergency or destitution, looking for missing persons, arrests, deaths or other emergencies, contact the closest U.S. Consulate.
http://travel.state.gov/travel/tips/emergencies/emergencies_1212.html

U.S. Passport replacement:
http://travel.state.gov/travel/tips/emergencies/lostpassport/lostpassport_1197.html

IMPORTANT CONTACT NUMBERS WHILE TRAVELING OVERSEAS

Defense Hotline Number
The Pentagon, Washington, DC 20301-1900
Tel. 800- 424-9098

Department of State Citizens Emergency Center Assistance to Travelers
(For current travel advisories)
Tel. 202-647-5225

International Association for Medical Assistance to Travelers
(for list of English-speaking doctors practicing in foreign countries)
Tel. 716-754-4883

U.S. Customs 24-hour Emergency Toll-Free Number
Tel. 800-522-5220

PURPOSE

As a cleared federal government contractor employee, you have access to critical corporate and U.S. Government information. The purpose of this briefing is to ensure that you understand your responsibilities to protect the information, and to make you aware of security vulnerabilities associated with foreign travel.

Presidential Decision Directive/NSC-12 "Security Awareness and Reporting Foreign Contacts" and NISPOM 10-604 require security personnel to establish and maintain security awareness programs which include formal briefings of the threat posed by foreign intelligence services. The awareness program must focus on the intelligence gathering of classified as well as other sensitive information.

APPLICABILITY

This briefing is applicable to all employees and consultants traveling internationally on behalf of the company.

AREAS OF INTEREST

As a cleared government contractor DynCorp International LLC (DI) has access to information of interest to foreign powers and entities whether it be classified, sensitive, proprietary or other information. Because of your access to personnel, facilities, and information, you present an opportunity for a foreign entity to expand their knowledge about U.S. technology, capabilities and vulnerabilities. The information contained in this briefing regarding possible intelligence collection may occur in any country, even in countries with which we are allies. For that reason, you must be alert to your surroundings and be aware of your actions at all times wherever you travel internationally.

CLEARED EMPLOYEES – TAKE NOTICE

Whether on official travel or vacation you have certain reporting and notification responsibilities as a result of your having access to classified information. Specifically:

- You must notify the DI Industrial Security Office (ISO) prior to any overseas travel.

- If you hold access to SCI, the agency sponsoring the SCI must also be notified in accordance with agency requirements. In some cases you may need to provide such notice at least 30 days before travel. The DI ISO will instruct you in your reporting responsibilities when you notify them of your travel plans.

THE NATIONAL SECURITY THREAT LIST

The FBI considers the following to be threats to our national security regardless of the country involved and includes any foreign intelligence activity which is:

- Targeting U.S. Intelligence and Foreign Affairs information and U.S. Government Officials
- Directed at the collection of critical U.S. technology
- 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 weapons of mass destruction

If you become aware of or suspect any foreign intelligence activity aimed at the above list notify your Facility Security Officer (FSO).

REQUIRED REPORTS

In accordance with Presidential Decision Directive/NSC-12 Security Awareness and Reporting Foreign Contacts and NISPOM 1-302b, contractors are required to report efforts by any individual, **regardless of nationality**, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported.

FEDERAL BUREAU OF INVESTIGATION: In accordance with the NISPOM, the FSO must promptly submit a written report to the nearest field office of the FBI and to DSS regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations.. Notification shall be made to your FSO.

DEFENSE SECURITY SERVICE: Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported to your FSO.

PRIOR TO DEPARTURE

1. Notify your FSO of your travel plans. Complete the Foreign Travel Notification Form.

2. Make two copies of your itinerary, passport data page, identification cards and visas if applicable. Leave one copy at home or with your supervisor. Keep the other copy with you but in a separate place than the originals. This will assist in the case of an emergency or loss of passport.

3. Ensure that items you carry with you are not controversial or prohibited. Political material or anything that could be considered pornographic should not be carried. If you carry prescription drugs with you, be certain that they are clearly marked and bring only necessary quantities. Some countries require a doctor's certification that prescription medication is required. Please contact the U.S. Department of State for country-specific instructions.

4. 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.

5. **DO NOT TAKE CLASSIFIED MATERIAL** with you as you travel. Arrange to have the material transmitted by other means prior to your departure. Consult with your FSO for guidance.

UPON ARRIVAL

1. An accurate declaration of all money and valuables should be made at the entry point. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. Keep receipts of all money exchanges as these may be required upon departure. Undeclared sums of U.S. or other currency may cause difficulty with authorities and could be confiscated upon departure.

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

YOUR ACTIVITIES AND BEHAVIOR

1. In all of your activities, show discretion and common sense. MAINTAIN A LOW PROFILE. 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.

2. Do not discuss classified or sensitive information in any vehicle, restaurant, hotel room, hotel lobby, or other public place. Your conversation may be overheard or you may be monitored.
3. 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 FSO.
4. Never leave luggage or briefcases that contain classified or sensitive information unattended. Keep briefcases or luggage containing sensitive information and company-issued electronics in your immediate possession. If you believe your luggage or briefcase has been searched, report the incident to your FSO when you return.
5. 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 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.
6. Never try to photograph military personnel, installations, or other "restricted areas". It is best to also refrain from photographing police installations, industrial structures, transportation facilities and boarder areas.
7. 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.
8. Do not accept packages and agree to transport them back to the U.S. Even if your friends, relatives, or professional contacts, make the request, do not accept the package.
9. If you will be on an extended visit and expect to be writing or receiving mail, remember that it may be subjected to censorship. Never make references to any classified or sensitive information.
10. Avoid any areas where there are demonstrations, protests or political/ or ethnic unrest.
11. Should you be detained or arrested for any reason by the police or other official, 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 a U.S. Embassy representative.
12. Do not leave documents in hotel safes.

UPON YOUR RETURN

Contact your FSO to report foreign contacts and any unusual incidents. You are required to report all contacts with individuals of any nationality, either within or outside the scope of your official activities, in which:

- Illegal or unauthorized access is sought to classified or sensitive information
- 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 so that they can be reached in the event of an emergency.

U.S. STATE DEPARTMENT RECOMMENDATIONS

- Sign up for the Smart Traveler Enrollment Program (STEP) so the U.S. Department of State (DoS) can better assist you in an emergency. This will help them contact you if there is a family emergency in the U.S., or if there is a crisis where you are traveling.
- Make sure you have a signed, valid passport, and a visa, if required, and fill in the emergency information page of your passport.
- Leave copies of your itinerary, passport data page and visas with family or friends, so you can be contacted in case of an emergency.
- Ask your medical insurance company if your policy applies overseas, and if it covers emergency expenses such as medical evacuation. If it does not, you may want to consider supplemental insurance.
- While in a foreign country, you are subject to its laws. The DoS web site at Country-Specific Information has useful safety and other information about the countries you will visit.
- To avoid being a target of crime, do not wear conspicuous clothing or jewelry and do not carry excessive amounts of money.

TRAVELING WITH LAPTOPS, PDAs AND OTHER ELECTRONIC DEVICES

From the National Counterintelligence Executive (www.ncix.gov)

YOU SHOULD KNOW…

- In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
- All information you send electronically – by fax machine, personal digital assistant (PDA), computer, or telephone – can be intercepted. Wireless devices are especially vulnerable.
- Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it is off. To prevent this, remove the battery.
- Malware can also be transferred to your device through thumb drives, computer disks, and other "gifts."
- Transmitting sensitive government, personal, or proprietary information from abroad is risky.
- Corporate and government officials are most at risk, but do not assume you are too insignificant to be targeted.
- Foreign security services and criminals are adept at "phishing" – that is, pretending to be someone you trust in order to obtain personal or sensitive information.
- If a customs official demands to examine your device or if your hotel room is searched while the device is in the room and you are not, you should assume the device's hard drive has been copied.

BEFORE YOU TRAVEL

- If you can do without the device, don't take it.
- Don't take information you don't need, including sensitive contact information.
- Consider the consequences if your information were stolen by a foreign government or competitor.
- Back up all information you take; leave the backed-up data at home.
- If feasible, use a different mobile phone or PDA from your usual one. Seek official cyber security alerts from: www.onguardonline.gov and www.us-cert.gov/cas/tips.

PREPARE YOUR DEVICE

- For Company-owned equipment check with IT
- For your personal equipment:
  - Create a strong password. Change passwords at regular intervals and as soon as you return.
  - Download current, up-to-date antivirus protection, spyware protection, OS security patches, and a personal firewall.
  - Encrypt all sensitive information on the device.
  - Update your web browser with strict security settings.
  - Disable infrared ports and features you don't need.

WHILE YOU'RE ON TRAVEL

- Avoid transporting devices in checked baggage.
- Use digital signature and encryption capabilities when possible. Do not use thumb drives.
- Do not leave electronic devices unattended. If you have to stow them, remove the battery and SIM card and keep them with you.
- Shield passwords from view. Do not use the "Remember Me" feature on many websites; retype the password every time.
- Terminate connections when you are not using them.
- Clear your browser after each use: delete history files, caches, cookies, URL, and temporary internet files.
- Don't open emails or attachments from unknown sources.
- Avoid Wi-Fi networks if you can. In some countries they're controlled by security services; in all cases they are not secure.
- If your company equipment is stolen, contact the Service Desk.
- If your personal device or information is stolen, report it immediately to the local U.S. embassy or consulate.

THREAT AWARENESS – PERSONAL SAFETY

TERRORIST ACTIVITY

Terrorist acts occur unpredictably, making it impossible to protect yourself absolutely. The first and best protection is to avoid travel to areas where there has been a persistent record of terrorist attacks or kidnappings. The following precautions may also provide some degree of protection and can serve as practical and psychological deterrents to would-be terrorists.

- Schedule direct flights, if possible, and avoid stops in high-risk airports or areas.
- Be cautious about what you discuss with strangers or what others may overhear.
- Try to minimize the time spent in the public area of an airport, which is a less protected area. Move quickly from the check-in counter to the secured areas. Upon arrival, leave the airport as soon as possible.
- As much as possible, avoid luggage tags, dress and behavior that may draw attention to you. *(i.e., shirts, caps or tags with the American flag on them)*
- Keep an eye out for abandoned packages, briefcases, or other suspicious items. Report them to airport authorities and leave the area promptly.
- Report any suspicious activity to local police and the nearest U.S. embassy or consulate.
- If possible, travel with others.
- Be sure of the identity of visitors before opening the door of your hotel room. Do not meet strangers at your hotel room or at unknown or remote locations.
- Refuse unexpected packages.
- Check for loose wires or other suspicious activity around your car.
- If you are ever in a situation where somebody starts shooting, crouch down on the floor. Do not move until you are sure the danger has passed. Do not attempt to help rescuers and do not pick up a weapon.

HIGHJACKING / HOSTAGE SITUATIONS

While every hostage situation is different, there are some general considerations to keep in mind. U.S. Government policy is firm: we do not make concessions to terrorists. When Americans are abducted overseas, we look to the host government to exercise its responsibility under international law to protect all persons within its territories and to bring about the safe release of hostages. We work closely with these governments from the outset of a hostage-taking incident to ensure that our citizens and other victims are released as quickly and safely as possible. At the outset of a terrorist incident, the terrorists typically are tense, high-strung and may behave irrationally.

- It is extremely important that you remain calm and alert and control your own behavior.
- Avoid resistance and sudden or threatening movements. Do not struggle or try to escape unless you are certain of being successful.
- Do not try to be a hero; you may endanger yourself and others.
- Consciously put yourself in a mode of passive cooperation. Talk normally. Do not complain, avoid belligerence, and comply with all orders and instructions.
- If questioned, keep your answers short. Do not volunteer information or make unnecessary overtures.
- Make a concerted effort to relax. Prepare yourself mentally, physically and emotionally for the possibility of a long ordeal.
- Try to remain inconspicuous, avoid direct eye contact and the appearance of observing your captors' actions.
- Establish a daily routine of mental and physical activity.
- Think positively and avoid a sense of despair. You are a valuable commodity to your captors, and it is important to them to keep you alive and well.

IF YOU ARE A VICTIM OF A CRIME WHILE OVERSEAS

Consular officers are committed to assisting American citizens who become victims of crime while abroad. Familiar with local government agencies and resources in the country where they work, consular officers can help American crime victims to:

- replace a stolen passport or address other emergency needs that arise as a result of the crime;
- contact family, friends, or employers;
- obtain appropriate medical care;
- provide information about the local criminal justice process and about the case itself;
- obtain information about local resources to assist victims, including foreign crime victim compensation programs; and
- obtain a list of local attorneys who speak English.

For more information about consular assistance for victims of crime abroad, see http://travel.state.gov/travel/tips/emergencies/victims_crime_overseas/victims_crime_overseas_1748.html

IF YOU ARE ARRESTED WHILE OVERSEAS

When you are in a foreign country, you are subject to its laws, and American officials are limited as to how they can assist you. They cannot, for instance, represent you in legal proceedings or pay your legal fees or other expenses. They can, however, perform a variety of vital services, which include provide a list of attorneys, assist in contacting your family in the U.S. if you desire, help you obtain money from family in the U.S., and monitor your health and welfare and the conditions under which you are being held.

If you are arrested, immediately ask to speak to a consular officer at the nearest U.S. Embassy or Consulate. If your request to speak to your consul is turned down, keep asking—politely, but persistently. For information on how consuls assist American arrestees, see http://travel.state.gov/travel/tips/emergencies/emergencies_1212.html.

IF YOUR MONEY OR PASSPORT IS LOST OR STOLEN

HOW TO ACCESS FUNDS IN THE U.S.

U.S. Consuls can assist Americans abroad who are temporarily destitute due to unforeseen circumstances. Americans who find themselves in these circumstances should contact the nearest U.S. Embassy or Consulate or the Department of State's Office of Overseas Citizens Services at 1-888-407-4747 (during business hours) or 202-647-5225 (after hours). Consular officers can help destitute Americans contact family, bank, or employer to arrange for transfer of funds. In some cases, these funds can be wired through the U.S. Department of State.

HOW TO GET YOUR PASSPORT REPLACED

If your U.S. passport is lost or stolen while you are overseas, report it immediately to the local police and to the nearest U.S. Embassy or Consulate. A consul can issue a replacement passport, often within 24 hours. If your U.S. passport is lost or stolen in the U.S., report it to the U.S. Department of State by following instructions found at http://travel.state.gov/passport/lost/lost_848.html. More information is available at http://travel.state.gov/travel/tips/emergencies/lostpassport/lostpassport_1197.html.

IMPORTANT CONTACT NUMBERS

Use this to list any emergency contact personnel. Take a copy with you and leave a copy with a family member or close friend in the U.S.

WHO?	HOW?
My Supervisor	Cell / Office / Home / Email
Family Member	Cell / Office / Home / Email
HR Representative	Cell / Office / Home / Email
Facility Security Officer	Cell / Office / Home / Email
	Cell / Office / Home / Email
	Cell / Office / Home / Email
	Cell / Office / Home / Email
	Cell / Office / Home / Email
	Cell / Office / Home / Email
	Cell / Office / Home / Email