AKIMA, LLC SECURITY GROUP

This briefing is applicable to all employees and consultants travelling internationally on behalf of the company. This is an annual requirement for employees who are required to travel internationally.

INTERNATIONAL TRAVEL SECURITY BRIEFING

What you need to know …

Table of Contents

[IMPORTANT RESOURCES FOR INFORMATION WHILE OVERSEAS 2](#_Toc322017738)

[IMPORTANT CONTACT NUMBERS WHILE OVERSEAS 2](#_Toc322017739)

[PURPOSE 3](#_Toc322017740)

[APPLICABILITY 3](#_Toc322017741)

[AREAS OF INTEREST 3](#_Toc322017742)

[CLEARED EMPLOYEES – TAKE NOTICE: 3](#_Toc322017743)

[THE NATIONAL SECURITY THREAT LIST 4](#_Toc322017744)

[REQUIRED REPORTS 4](#_Toc322017745)

[PRIOR TO DEPARTURE 5](#_Toc322017746)

[UPON ARRIVAL 5](#_Toc322017747)

[YOUR ACTIVITIES AND BEHAVIOR 6](#_Toc322017748)

[UPON YOUR RETURN 7](#_Toc322017749)

[EMERGENCY NOTIFICATION PHONE NUMBERS 7](#_Toc322017750)

[THE STATE DEPARTMENT RECOMMENDS… 7](#_Toc322017751)

[TRAVELLING WITH LAPTOPS, PDAS AND OTHER ELECTRONIC DEVICES: 9](#_Toc322017752)

[THREAT AWARENESS – PERSONAL SAFETY 10](#_Toc322017753)

[TERRORIST ACTIVITY 10](#_Toc322017754)

[HIGHJACKING / HOSTAGE SITUATIONS 10](#_Toc322017755)

[IF YOU ARE A VICTIM OF A CRIME WHILE OVERSEAS: 11](#_Toc322017756)

[IF YOU ARE ARRESTED WHILE OVERSEAS: 11](#_Toc322017757)

[IF YOUR MONEY OR PASSPORT IS LOST OR STOLEN: 12](#_Toc322017758)

[HOW TO ACCESS FUNDS IN THE U.S. 12](#_Toc322017759)

[HOW TO GET YOUR PASSPORT REPLACED 12](#_Toc322017760)

[IMPORTANT CONTACT NUMBERS I WILL NEED WHILE I AM AWAY. 12](#_Toc322017761)

[WHO? 12](#_Toc322017762)

[HOW? 12](#_Toc322017763)

IMPORTANT RESOURCES FOR INFORMATION WHILE OVERSEAS

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/emergencies_1748.html>.

Financial emergencies or destitution: <http://travel.state.gov/travel/tips/emergencies/emergencies_1198.html>

Obtaining funds from the U.S. (OCS trust): <http://travel.state.gov/travel/tips/brochures/brochures_1224.html>

Missing persons: <http://travel.state.gov/travel/tips/emergencies/emergencies_1195.html>

Arrests: <http://travel.state.gov/travel/tips/emergencies/emergencies_1199.html>

Deaths: <http://travel.state.gov/travel/tips/emergencies/emergencies_1205.html#death>

Passport replacement: <http://travel.state.gov/travel/tips/emergencies/emergencies_1197.html>

IMPORTANT CONTACT NUMBERS WHILE OVERSEAS

Defense Hotline

The Pentagon Washington, DC 20301-1900 (800) 424-9098

Department of State Citizens Emergency Center Assistance to Travelers

(For current travel advisories) (202) 647-5225

International Association for Medical Assistance to Travelers

(For list of English-speaking doctors practicing in foreign countries) (716) 754-4883

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

PURPOSE

As a federal 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” requires 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 travelling internationally on behalf of the company. This is an annual requirement for employees who are required to travel internationally.

AREAS OF INTEREST

As a cleared government contractor we have access to information of interest to foreign powers and entities whether it be classified, sensitive, proprietary or other information of interest. 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 countries with which we are allies. For that reason, we **a**sk you to be alert to your surroundings and aware of your actions at all times wherever you travel internationally.

CLEARED EMPLOYEES – TAKE NOTICE:

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

* You must notify your security office prior to any overseas travel and receive a copy of this briefing booklet.
* If you hold access to SCI – you MUST notify the agency sponsoring the SCI in accordance with agency requirements. In some cases you may need to provide such notice at least 30 days before travel. This is in addition to notification requirements to the company security office.

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 critical 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 special weapons of mass destruction

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

REQUIRED REPORTS

In accordance with Presidential Decision Directive/NSC-12 Security Awareness and Reporting Foreign Contacts, 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, we must promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. Reports can be made directly to the FBI by contacting any local FBI Field Office. Notification should also be made to your Facility Security Officer.

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. Contact your Facility Security Officer for assistance and to make reports.



PRIOR TO DEPARTURE

1. All international travel conducted on behalf of the company must be pre-approved by the employee’s supervisor and in accordance with the corporate policy on international travel. Caution must be exercised to ensure that travel plans and purposes are submitted for approval as early as possible so as not to interfere with actual travel plans.

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.

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 Security Officer for guidance.

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

7. Ensure that proper notifications have been made to supported agencies. As an example, if you are under contract to support a federal agency, be sure to follow the guidelines established by that agency regarding foreign travel. If you hold SCI / SAP or other sensitive information access, your notifications will need to be made to your granting agency well in advance of your planned trip.

UPON ARRIVAL

1. 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; 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.

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. In any 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 security officer.

4. Never leave luggage or briefcases that contain classified or sensitive information unattended. This includes leaving your briefcase in your hotel room. We encourage you to keep your briefcase containing sensitive information, immediately in your possession. Personnel frequently report occurrences of their luggage or briefcase being searched or rummaged through. If this happens to you, report the incident to your Security Officer 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, and 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 is political or ethnic unrest, demonstrations or protests.

11. 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.

12. Do not leave documents in hotel safes.

UPON YOUR RETURN

Contact your Security Officer to report foreign contacts and any unusual incidents. You must receive a security debriefing if you have been abroad for more than 90 days. 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 you can be reached in the event of an emergency. If this is not possible, the 24-hour State Department Operations Center at 202-647-1512, may be able to assist others in reaching you.

THE STATE DEPARTMENT RECOMMENDS…

* Sign up for the Smart Traveler Enrollment Program so the State Department can better assist you in an emergency at [https://travelregistration.state.gov](https://travelregistration.state.gov/). 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, consider supplemental insurance.
* While in a foreign country, you are subject to its laws. The DOS web site at [Country Info](http://travel.state.gov/travel/cis_pa_tw/cis/cis_1765.html) 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. Also, do not leave unattended luggage in public areas and do not accept packages from strangers.

TRAVELLING WITH LAPTOPS, PDAS AND OTHER ELECTRONIC DEVICES:

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

**WHILE YOU’RE AWAY**

* Avoid transporting devices in checked baggage.
* Use digital signature and encryption capabilities when possible. Don’t use thumb drives.
* Don’t 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. Don’t use the “Remember me” feature on many websites; re type the password every time.
* Terminate connections when you’re 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’re insecure.
* If your device or information is stolen, report it immediately to your home organization and the local US embassy or consulate.

**PREPARE YOUR DEVICE**

* 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.

**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](file:///E:\Travel%20Stuff\www.onguardonline.gov%20and%20www.us-cert.gov\cas\tips)

**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’s off. To prevent this, remove the battery.
* Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other “gifts.”
* Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.
* Corporate and government officials are most at risk, but don’t assume you’re 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’re not, you should assume the device’s hard drive has been copied.

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. These precautions may 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.
* Keep an eye out for abandoned packages or 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. Don't 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, drop to the floor or get down as low as possible. Don't 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.
* Don't try to be a hero, endangering yourself and others.
* Consciously put yourself in a mode of passive cooperation. Talk normally. Do not complain, avoid belligerency, and comply with all orders and instructions.
* If questioned, keep your answers short. Don't 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 program 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/emergencies_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 providing a list of attorneys, assisting in contacting your family in the U.S. if you wish it, helping you obtain money from family in the U.S., and monitoring 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_1199.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 (see [http://usembassy.state.gov](http://usembassy.state.gov/) for contact information) or the State Department’s Office of [Overseas Citizens Services](http://travel.state.gov/travel/about/about_1245.html) 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 Department of State. For information on how a consular officer can help under these circumstances, see <http://travel.state.gov/travel/tips/emergencies/emergencies_1198.html>.

## 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. Links to contact information for U.S. Embassies and Consulates may be found at [http://usembassy.state.gov](http://usembassy.state.gov/). If your U.S. passport is lost or stolen in the U.S., report it to the Department of State by following instructions found at <http://www.travel.state.gov/passport/lost/lost_848.html>. More information is available at <http://travel.state.gov/travel/tips/emergencies/emergencies_1197.html>.

## IMPORTANT CONTACT NUMBERS I WILL NEED WHILE I AM AWAY.

Use this to list any emergency contact personnel.

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

**TRAVEL BRIEFING ACKNOWLEDGEMENT**

My signature below indicates that I have read, been briefed, and understand the International Travel Security Briefing information provided to me. I am aware that any questions I have concerning the contents of this briefing should be directed to my immediate supervisor or to the company Facility Security Officer.

|  |  |
| --- | --- |
| Name (First, Middle, Last) |  |
| Social Security Number (Last 4 numbers) |  |
| Company |  |
| Travel Date(s) |  |
| Country/Region |  |
| Work Number |  |
| Cell Phone Number |  |
| Email |  |

*Please provide a copy of the signed acknowledgement to your security officer.*

Signature Date

RECORDS RETENTION: *Security*: Retain signed copies of this acknowledgement in the individual’s personnel security file.

TRAVEL OUT-BRIEFING

|  |  |  |
| --- | --- | --- |
| *To conducted upon your return, however if anything suspicious happens during your travel please contact your security officer immediately.* | YES | NO |
| 1. Were any problems encountered at the time of arrival or departure from the foreign country/countries visited? If YES please explain: |  |  |
| 2. Did you have any unusual experiences while traveling to include harassment, suspected surveillance, detention, unusual customs inspection, searches of hotel room or trash, listening devices found, telephone monitoring? If YES please explain: |  |  |
| 3. Any travel restrictions imposed by the country during your visit? Were there any abrupt changes made in the itinerary? If YES please explain: |  |  |
| 4. Were any probing inquiries made relative to your job duties, studies, and/or company or organization? If YES please explain |  |  |
| 5. Were there any blatant indications of possible approach/efforts to compromise by a foreign intelligence service? If YES please explain: |  |  |
| 6. Did you meet a foreign national who requested future contact? If YES please explain: |  |  |
| 7. Were you a victim of a criminal act? If YES please explain: |  |  |
| 8. Were you detained or arrested? If YES please explain: |  |  |
| 9. Did you witness any acts that may be considered terrorist-like? If YES please explain: |  |  |
| 10. Were you approached by anyone offering to exchange currency? If YES please explain: |  |  |
| 11. Did you lose/misplace any official materials or personal luggage? If YES please explain: |  |  |
| 12. Did you take any personal pictures of foreign government, military installations, or equipment? If YES please explain: |  |  |
| ***Additional information may be requested based on the information provided above. Your security officer will advise if this is necessary.***  Out brief completed by: Your Printed Name: Date: | | |