U.S. Department of Commerce
Office of Security

Foreign Travel Briefing

CLASSIFICATION: UNCLASSIFIED BRIEFING

Derived from open source material

Overseas Travel Briefing

The security and safety measures suggested here will help protect you from crime, terrorism, and actions by foreign intelligence and security organizations, while traveling for the Government.

The level and type of threat varies depending on the Country and political climate, so use your best judgment when choosing which of these measures to implement.

Country Specific Threat Updates:

The Department of State (DOS), Bureau of Consular Affairs maintains travel warnings and Consular information sheets with rules and regulations pertaining to foreign travelers for every country in the world at:

http://www.travel.state.gov

Classified, country-specific threat briefs can be arranged through the Department of Commerce's Office of Security.

Some Countries have **import restrictions** or **prohibit** the entry/use of encryption programs within their borders. Check the above State Department web site for more information.

Understanding the Information Technology (IT) Threat

First, understand that the threat is <u>real!</u> Examples of reported incidents include:

-Unauthorized full disk copies have been made while the laptop owner was out of the hotel room on overseas travel.

-Laptops have been stolen at security screening lines at airports.

-Wireless access services have been monitored by third parties to gain information transmitted through WiFi service.

-Malicious software installations have occurred including viruses, Trojan horses, Key loggers; and programs that capture log-in data and automatically transmit key data to other locations.

DOC IT Travel Policy

- Permanent-issued DOC laptops that connect to Operating Unit networks and personal laptops are **prohibited** from use while on official foreign travel.

- Only Operating Unit issued loaner laptops are authorized during foreign travel.

  -Loaner laptops should only be utilized on foreign travel when there is an official business need.

  -Using the loaner laptop, only remote access via Operating Unit internet based e-mail, or issued MobiKey (if available) will be permitted during foreign travel.

DOC IT Travel Policy

- DOC personnel must have their Blackberries evaluated before and after foreign travel by their Operating Unit IT office for adequate security controls:

  -At least 72 hours prior to travel, and again within the first business day upon return, prior to connecting the device to a networked computer.

- OS Blackberry users with a security clearance may contact (202) 482-5344 to view a video on protective techniques.

- If your Blackberry is ever lost or stolen, immediately report the incident to your Operating Unit IT Security Officer.

IT Security

- Make sure your use of Government Furnished Equipment (GFE) and Commerce data is used and secured in accordance with the Commerce IT Security Program Policy and Minimum Implementation Standards.
- Gain supervisor approval to remotely use and/or access sensitive information.
- Attend Commerce sponsored IT security awareness training to ensure you understand threats affecting the security of Commerce systems and data.
- Only transport electronic devices containing Commerce information when absolutely required for use during travel.
- Each Operating Unit is required to set up a loaner laptop program for overseas use. These laptops will be sanitized after each use.
- No sensitive data is authorized for storage on loaner laptops.
- NEVER store passwords, sign-on sequences or access phone numbers on any device or in its case.

IT Security

- For any non-sensitive data being loaded on loaner laptops, ensure information is “backed-up” prior to travel.
- Create strong and unique passwords, and shield passwords from view when inputting.
- Be aware of shoulder surfing when viewing device monitors or reading non-digital documents.
- Run up-to-date anti-virus software, anti-spyware, and personal firewalls on laptops used for all travel.
- Terminate connections when not in use.
- Clear browser history and cache after use, and close browser.
- Implement “full disk” encryption for portable electronic devices when traveling abroad.
- Maintain physical control of laptop computers and other electronic devices when traveling abroad.
- Minimize the data stored on electronic devices used when traveling abroad, and do not store sensitive data on loaner laptops.

IT Security

- When using portable thumb drives for data storage, ensure that the device is secure using FIPS 140-2 encryption technology to protect data.
- Inventory what is loaded (software, data, etc) on the loaner laptop or other electronic devices prior to departure and after return from travel abroad.
- Do not loan your laptop to anyone when traveling abroad. An innocent connection to an IT system or website could result in malware being loaded on your computer.
- Minimize web-browsing while traveling abroad and when using a non-Commerce managed web service.
- Do not use overseas Wireless (WiFi) public use service to connect to Commerce systems (i.e. do not check your mail or access DOC business systems using a WiFi service where sniffing or key-logging can take place).
- Disable the Infrared port (i.e. cover it with a piece of black electrical tape, or disable via the BIOS) on portable electronic devices.
- Refrain from taking personal laptops, cell phones, PDA’s and other like items as these devices also become a target for malicious use or hacking.

Reporting IT-Related Incidents

- It is Commerce policy that you report any incident relating to Information Technology, including data compromise and loss of equipment such as laptops, Blackberry, DOC issued cell phones, thumb drives, etc…to your respective organization's IT Security Officer immediately after you confirm or suspect a compromise. You should note that you cannot wait until you return from travel to file a report. Your agency's Computer Incident Response Team will ensure that reported information is properly managed and addressed.

Pre-Travel Preparations:

- To avoid attracting criminal interest, dress discreetly and appropriately to blend with the local culture, avoid the appearance of wealth and consider not wearing jewelry or expensive watches.

- Obtain a modest sum of money before you leave home; criminals watch for travelers exchanging large amounts of currency at airport banks or currency exchange windows.

- While traveling abroad, you will frequently find yourself in unfamiliar places, not knowing the local customs and language. Thus, you may become a promising **target** for local criminals who are looking for an **easy mark**.

- **The best countermeasure against this is increased personal awareness. Prior planning, regular use of good security and safety measures, awareness of your environment and some basic common sense can effectively protect you.**

Pre-Travel Preparations:

- Check your wallet/purse and remove all credit cards, social security cards, Military reserve ID and other non-essential papers that are not needed for your trip.

- Include an **Emergency Information Card** which has your name, blood type, known allergies, required medications, insurance information and emergency contact information.

- Make copies of your passport (photo page, VISA page, and any amendments), ticket, credit cards and other documents you need to take with you. Leave a copy with someone in the United States who is **not** traveling with you, and carry a copy to facilitate replacing any lost items.

Pre-Travel Preparations:

When traveling abroad, the odds are in your favor that you will have a safe and incident free trip. However, you should prepare yourself for all possibilities.

It seems impossible, but consider what would happen if you became a victim of a hijacking, kidnapping, other hostage situation, or found yourself in the middle of civil unrest.

Are your personal affairs in order? Do you have a will (with MIA clause), Living Will, Power of Attorney (Financial and Medical), long-term Child care or Custody Agreement?

•**All Americans should intensify personal safety practices while on travel outside the United States.**

Pre-Travel Preparations:

- Carry all your prescriptions (in their original bottles), an extra pair of eye glasses/contacts, a change of clothes and your personal document copies in your carry-on luggage.

- Luggage tags should be closed and only show your name, phone number and address (work is recommended). Avoid using a business card, logos, stickers or seals which could disclose an affiliation.

- Use hard, lockable luggage with a Transportation Security Administration (**TSA) approved lock** (deters petty intrusions).

At the Airport

- Protect yourself from petty theft. Keep your luggage within view at all times. Watch for distractions which could be used as an opportunity for pickpockets or thieves.

- If you are traveling with a laptop, cell phone or PDA treat it as a wallet/purse and carry it on the plane with you. Portable electronic devices are **regularly** targeted by **thieves** (cash value) and **Foreign Intelligence services** (information value). Take only the required electronic equipment with you on your trip.

- At the airport, maintain a low profile. Once you have checked in, immediately proceed through security, as it is the safest area in the airport.

- While at security, prior to placing your items on the x-ray machine, ensure there are no other individuals holding up the line, and ensure you have removed all metal from your pockets. You want to proceed through and re-claim your carry-on luggage as quickly as possible. If there is a problem at the checkpoint, wait for it to be resolved before placing your carry-on through the x-ray.

- Airport departure tax varies from Country to Country. Often it is included in the price of the ticket. Sometimes, however; the traveler must pay in local currency at the airport. **Know before you go!**

In Transit

- Upon arrival at your destination, claim your luggage and depart the airport as quickly as possible.
- **Never take a gypsy taxi!** Always use an approved taxi from an official stand, if possible.
- If you are renting a car, arrange in advance for a conservative car. Upscale vehicles are frequently targeted by carjackers. Never store any items in plain sight. If the vehicle must be left unattended, place luggage and laptops in the trunk whenever possible.
- Know your route! Obtain maps and directions in advance, before leaving the rental agency.
- Drive defensively and avoid getting boxed in. If threatened, do not be afraid to floor it to get away and out of the area.
- Travel in pairs, when possible. Avoid alleys and short-cuts. Consider taking a taxi to your destination if you must travel alone after dark. Avoid parking in unlit lots or along dark streets.

At the Hotel

- Remain with your luggage until it is either turned over to a hotel bellman, or stored safely in your room.
- In many Countries, you will be asked to surrender your passport when registering at a hotel. This is a **routine procedure**, as many hotels must submit a daily report to police on all registered guests. Be aware that this information may be reviewed by the local intelligence service!
- Don't forget to get your passport back at the earliest opportunity.
- Once inside your hotel room, use all of the locking devices on doors and windows.
- Remember the hotel emergency key can override your deadbolt.
- Do not advertise your absence with "Service this room now" sign.
- Keep your room key with you at all times.

At the Hotel

- Do not use your name when answering your room phone.
- Never accept any packages at your room or open the door for workmen or other unknown individuals without prior verification from the front desk.
- Keep your luggage locked when you are out of your room. This won't stop a professional, but will keep the curious maid honest.
- At night, or when in the shower, lock your valuables in your suitcase or room safe. This reduces the risk of mysterious disappearances while you are sleeping or in the shower.
- Consider bringing a flashlight. Emergency power and emergency lighting often do not exist in hotels in developing countries.

At the Hotel

- Documents and storage devices (thumb drive, hard drive, etc.) that could be of value to an intelligence service should be kept on your person at all times.
- Hotel rooms, telephones, and fax machines may be monitored, and personal possessions in hotel rooms, **including computers and PDA's**, may be searched (**and copied**) without the consent or knowledge of the traveler.
- Review local maps and become familiar with the area. Know the approximate locations of safe havens in the area (local Police Stations, hospitals, friendly country Embassy's, etc).
- Ask the front desk or concierge for help reading local maps, finding locations or getting directions. If using local transportation, ask the hotel staff to write out your destination and the hotel's address in the local language.
- Know how to utilize the local telephones and obtain change from the hotel, before departing.

In Public

- Inspect your credit card after each use and ensure that it is yours.
- Use caution when using Automated Teller Machines (ATM) overseas. Attempt to utilize an ATM at your hotel, at a bank, or other secured location. If your card is not returned, look inside the slot and to see if there is an obstruction and attempt to free your card. Under no circumstances should you provide your pin number to a bank employee or a "Good Samaritan" who may try and assist you.
- Consider carrying your wallet, passport and other valuables in your front pocket to make it more difficult for a pickpocket. Carry some smaller bills in a separate pocket to hand quickly to appease a mugger.
- Avoid street demonstrations. If overtaken, seek refuge in the nearest safe haven, Police or Fire station, hotel or department store.
- In the event of major civil unrest, remain in your hotel room. Ensure the Embassy is aware of your location. Stay away from windows and exterior walls.

Anti-Terrorism

Anti-Terrorism is a collection of defensive measures implemented to reduce the vulnerability of people, their property and institutions from terrorist attacks.

The threat of terrorism must be taken seriously by all Americans, especially those who travel regularly.

In comparison to all the other threats addressed, your greatest and most immediate threat to a safe trip is common criminal activity.

Terrorism 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 acts or kidnappings.

Most terrorism attacks are the result of careful planning. In addition, many terrorist groups, seeking publicity for political causes within their own country may not be looking for American targets.

Hijacking

Hijackings (or hostage) situations are **extremely rare**, but they do happen.

Either way, how **you** react during the first few minutes, may be crucial to the outcome.

- Schedule direct flights if possible and avoid stops in high-risk airports or areas.
- Be cautious about what you discuss with strangers.
- At the outset of a terrorist incident, the terrorists are typically tense, high-strung and may behave irrationally. It is extremely important that you remain **calm, alert and manage your own behavior**.
- Avoid resistance and sudden or threatening movements. Do not try to struggle or escape unless you are **certain** of being successful. Don't try to be a hero, endangering yourself and others.

Hijacking

- If questioned, keep your answers short. Do not volunteer information. Make a concerted effort to relax.
- Consciously put yourself in a mode of passive cooperation. Talk normally. Do not complain, avoid belligerency and comply with all orders and instructions.
- Try to remain inconspicuous. Avoid direct eye contact and the appearance of observing your captors actions.
- Remember that all hijackers / terrorists may not reveal themselves initially; some may wait **quietly** to react to events.
- If you are involved in a lengthy drawn out situation, try to establish a rapport with your captors, avoid political discussions or other confrontational subject.
- Establish a daily program of physical and mental activity. **Think positive!**

Hijacking

- If hijacking/hostage negotiations are successful, the terrorists may simply surrender to authorities, release all the hostages, or simply abandon the siege without incident.

- If not, a rescue force may attempt to resolve the situation. You should be prepared for this possibility and take the following precautions:

  -If you hear shots, immediately take cover

  -Remain calm and do not move, unless you are in imminent danger.

  -You do not want to be mistaken for a hijacker.

  -If fire or smoke appears, quickly move to the nearest exit.

  -Follow all instructions given by the rescue force.

  -On a tarmac, if not directed, quickly move away from the plane, toward the terminal or control tower.

- **You** may be treated as a hijacker until your identity is confirmed.

Counterespionage

- Aside from being a potential intelligence target for the information you possess, foreign government scrutiny of you in another country may also occur by design or chance for some of the following reasons:
  - Fitting a terrorism, narco-trafficking, criminal or other profile.
  - Involvement in black-market activity.
  - Discovery by the host nation government of material on your person or in your luggage that is banned or strictly controlled.
  - Associating with individuals the government labels as dissidents.
  - Having language fluency, declared relatives, or organizational affiliations in the country you are visiting.
- Usually, any foreign intelligence activities directed against you will be conducted in an unobtrusive and non-threatening fashion, although in some cases a foreign intelligence service may employ more aggressive tactics. While most harassment incidents are intentionally obvious – meant to intimidate or "test" a traveler's reaction – many intelligence activities are conducted without the targets awareness.

Counterespionage

- Some of the methods used to target travelers are:
- **Elicitation** – a ploy whereby seemingly normal conversation is contrived to extract information about individuals, their work or colleagues (designed to put you at ease and is difficult to recognize as an intelligence technique).
- **Eavesdropping/"Shoulder-Surfing"** – listening to your conversation to gather information.
- **Technical eavesdropping** – use of audio/video devices.
- **"Bag Operations"** – surreptitious entry into someone's hotel room to steal, photograph, or photocopy documents, steal or copy magnetic media or download from a laptop computer.
- **Electronic Interception** – increasingly conducted against modern telecommunications systems.
- **Overt theft** of your property.

Counterespionage

- Terrorists and spies share many traits. Some highlights of what you need to be aware of appear below. Both groups may:

  -Conduct surveillance
  -Make concerted collection efforts to gather intelligence
  -Approach you!
  -Attempt to recruit you!
  -Attempt to exploit you or your vulnerabilities or weaknesses
  -Attempt to place you in a position in which you feel threatened, "trapped" or uneasy.

- Travelers should be very cautious of Foreign Nationals, of the opposite sex, who attempt to **establish a relationship** or extend an **offer of companionship** to you. Often this is done to put the traveler in a compromising position.

- Travelers need to be conscious of Foreign Nationals who attempt to approach them to establish a **friendship** or **"practice the English language".** Although there are instances of this being an innocent event, the possibility exists that you may be a "target", and information may be solicited from you unwittingly.

Counterespionage

•Travelers need to be aware that although Foreign Nationals are employed by the U.S. Embassy, they are not necessarily cleared for sensitive conversations.

•Do not divulge information to anyone not authorized to hear it.

•While traveling abroad, you are on the host country's home turf, where the intelligence and security services of foreign governments have many resources available.

•They can **monitor** and, to some extent, **control** the environment in which you live and do your work.

•The Intelligence services of rival and friendly countries are now more active in collection operations against the United States than during the cold war.

•America's role as the dominant political, economical, and military force in the world makes it the **Number One target** for foreign intelligence collection.

Counterespionage

- Maintain control of sensitive documents or equipment. Keep unwanted material until it can be properly disposed of. Never leave these items unattended in your hotel room or hotel safe.
- Hotel rooms, commercial airlines, or other public places are **rarely suitable** to discuss sensitive information.
- Do not use your computer or fax equipment at hotels or business centers for sensitive matters.
- Taking photographs of anything that could be perceived as being of military or security interest may result in problems with authorities.
- While traveling abroad, all Americans should exercise caution in their **actions** and **activities**. Expect that your activities and actions are being **monitored** and avoid putting yourself in a position to have a weakness or vulnerability exploited.

Counterespionage

•As an American government official with access to useful information, **YOU** could become the **target** of a foreign intelligence operation at any time.

•Depending on your assignment, the risk of becoming an intelligence target may be ever present, but can increase greatly during foreign travel.

•Common sense and basic counterintelligence awareness can offer protection against attempts to collect classified, proprietary, privileged, and other types of sensitive material.

TRUST YOUR SECURITY INSTINCTS!

Reporting Incidents

- Reporting security incidents or suspected incidents is crucial. Reporting the incident **should be done at the earliest opportunity!**

- When overseas, security incidents should be reported to the U.S. Embassy Regional Security Officer (RSO), **through the nearest U.S. Diplomatic facility.** Remember that **telephone calls** to the local American Embassy or Consulate may be monitored by foreign intelligence and security services.

- After returning from your trip, any suspicious or noteworthy incidents need to be immediately reported to your organization's appropriate security component **and** to the Office of Security.

- Report any counter intelligence incident to the RSO, the relevant U.S. Government Agency, your Security Coordinator and the Office of Security at (202) 482-2942.

When in doubt, **REPORT IT!!!**

Country Specific Briefing -- China

- Travelers should respect local police requirements to avoid travel in some areas.
- Security personnel **may at times** place foreign visitors under **surveillance**.
- Foreign government officials, journalists, and business **people with access to advanced proprietary technology** are particularly likely to be under surveillance.
- In China, it is illegal to exchange dollars for RNB except at banks, hotels, and official exchange offices.
- Terrorism is rare in China, although a small number of bombings have occurred in areas throughout China.
- Travelers are subject to host Nation laws and must be familiar with them.
- Hotel rooms, telephones, and fax machines may be monitored, and personal possessions in hotel rooms, including computers, may be searched without the consent or knowledge of the traveler.

Country Specific Briefing -- China

- Over the past year, incidents of violence against foreigners, including sexual assaults, have taken place, usually in urban areas where bars and nightclubs are located.

- Caution should be exercised when visiting bar districts late at night, especially on weekends. There have been reports of bar fights in which Americans have been specifically targeted due their nationality.

- There has been an increase in the number of Americans falling victim to scams involving the inflation of tea and drink prices.

- Recently, American visitors have encountered scams at the international airport in China, whereby individuals appearing to work for the airport offer to take American tourists' bags to the departure area, but instead they carry the bags to another area and insist that the visitor pay an airport tax. Travelers need to be advised that the airport tax is included in the price of the airline ticket.

- Taking photographs of anything that could be perceived as being of military or security interest may result in problems with authorities.

Country Specific Briefing -- Venezuela

- ***The U.S. Embassy must approve <u>IN ADVANCE</u> the official travel to Venezuela of all U.S. Government personnel.***

- Because of the frequency of robberies at gunpoint, travelers are encouraged to arrive during daylight hours. If not, travelers should use extra care both within and outside the airport.

- The Embassy strongly advises that all arriving passengers make advance plans for transportation from the airport to their place of lodging. If possible, travelers should arrange to be picked up at the airport by someone who is known to them.

- Travel to and from Maiquetía Airport, the international airport serving Caracas, can be dangerous and corruption at the airport itself is rampant. Due to the poor security situation, the Embassy does not recommend changing money at the international airport.

- Kidnapping is a particularly serious problem.

Country Specific Briefing -- Venezuela

- Violent crime in Venezuela is pervasive, both in the capital, Caracas, and in the interior. The country has one of the highest per-capita murder rates in the world.
- Virtually all murders go unsolved.
- Armed robberies take place in broad daylight throughout the city, including areas generally presumed safe and frequented by tourists.
- Travelers should respect and know local police requirements and U.S. Embassy restrictions on avoiding travel in some areas.
- Foreign exchange transactions must take place through exchange houses or commercial banks at the official rate. **The Embassy cannot provide currency exchange services**. Currency exchange for tourists can be arranged at "casas de cambio" (exchange houses) -- located near most major hotels. Due to currency regulations, hotels cannot provide currency exchange. Exchanges through commercial banks must first be approved by the Commission for Administration of Foreign Currencies (CADIVI); and require a registration process, which delays the exchange.

Country Specific Briefing -- Venezuela

- Travelers are subject to host Nation laws and must be familiar with them.
- Laws issued by President Chavez under this authority (Rule by Decree) become effective immediately after their publication in the government legislative gazette. **As a result, laws directly impacting U.S. Citizens or their interests in Venezuela may come into force with little or no warning**.
- U.S. Citizens are advised to **carefully monitor changes** in Venezuelan law.
- Harassment of U.S. citizens by pro-government groups, Venezuelan airport authorities, and some segments of the police occurs but is quite limited. Venezuela's most senior leaders, including President Chavez, regularly express anti-American sentiment. The Venezuelan government's rhetoric against the U.S. government, its American culture and institutions, has affected attitudes in what used to be one of the most pro-American countries in the hemisphere.

If You Are Arrested or Detained:

- **Stay calm**, maintain your dignity and **do not do anything to provoke the arresting officers**.
- **Request to contact the nearest U.S. Embassy or Consulate.** If refused, **continue** to make requests periodically.
- Do not admit to anything or volunteer any information.
- Do not sign anything; **Politely** decline until the document can be examined by an attorney or representative from the U.S. Embassy or Consulate.
- Remember, while in a Foreign Country, you are subject to their laws and they may be very different from U.S. laws and regulations.

Resources

- Classified, country-specific threat briefings can be arranged for by contacting the Department of Commerce's Office of Security at (202) 482-2942.

- If you have questions about this briefing or need to report any suspicious activity promptly contact the Department of Commerce, Office of Security, at (202) 482-2942

CERTIFICATE

- To complete the training and receive credit, click on the link below to enter your personal information, complete the 5-question examination and receive a certificate for the completed training.
- **By clicking on the link below you are certifying that you have read the Defensive Travel Briefing.**

Click Here to get your Travel Briefing Certificate!

- You can also copy and paste the following link into your Web browser:
  https://securityexchange.osec.doc.gov/surveys/XA3EGA
- This briefing is valid for a period of one (1) year

Have a safe and secure trip!