Counterintelligence Support to Foreign Travel

Official foreign travel is utilized now more than ever to advance the Department of Energy's program objectives and mission. International interaction and cooperation can contribute to scientific breakthroughs and technological advances. However, increased interaction also means a greater risk of foreign intelligence collection activities. As a U.S. traveler, you may be the target of a foreign intelligence service seeking to overtly or covertly collect U.S. technological and/or proprietary information. In order to protect you, as well as our national interests, specific DOE requirements and guidelines for foreign travel have been created. This fact sheet addresses the counterintelligence part of the foreign travel authorization process. For complete information, refer to the DOE Order O551.1.

How does the Office of Counterintelligence help make foreign travel safe?

The Department of Energy's Order O551.1 -- "Official Foreign Travel" -- requires all employees and contractors to complete pre- and post- trip briefings when travelling to sensitive foreign countries. This policy is designed to protect national security interests as well as your own personal interests.

The specific actions you must take before and after travelling to a sensitive foreign country include:

- Schedule a pre-travel counterintelligence briefing with your local Office of Counterintelligence before leaving.
- Report any suspicious incidents to the Office of Counterintelligence immediately.
- Participate in a debriefing with your local counterintelligence officer (CIO) when you return from travel.

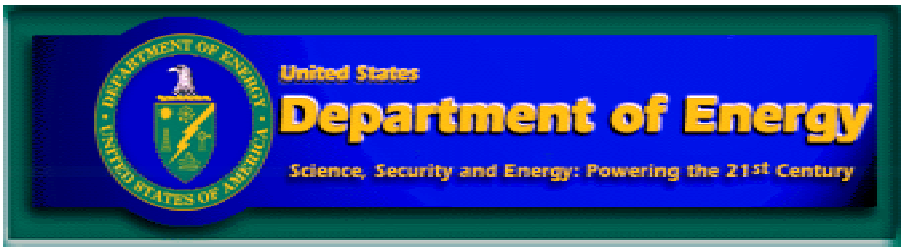
Pre-travel briefings inform individuals about what to guard against and what to expect when travelling to sensitive foreign countries. They are important for your personal safety as well as the safety of the information you carry. Your counterintelligence officer (CIO) will provide you with helpful tips for making sure that you are keeping yourself safe and protecting the information you hold.

The post-travel debriefing allows the Office of Counterintelligence to learn from your experiences while on travel, and use that information to enhance the effectiveness of future pre-briefings. Because U.S. citizens are often targeted by foreign intelligence services, it is necessary for you to be aware of the tactics used to obtain information. You are encouraged to talk to your CIO about the details of any unusual events encountered while on foreign travel.

As employees and contractors of the Department of Energy, your actions matter. Your attention to counterintelligence concerns and your proactive approach in sharing information with your counterintelligence officer will determine how well your interests, and our national security, are protected. The more information you have regarding elicitation methods and recruitment precautions the better protected you are against possible foreign intelligence threats.

What are the methods used by foreign intelligence services to obtain information from US travelers?

- **Elicitation:** An effort in which a seemingly normal conversation is contrived to extract information about individuals, their work, and their colleagues.



- **Eavesdropping:** Gathering information in social environments by listening in on private conversations.
- **Bag Operations:** Efforts to steal, photograph, or photocopy documents, magnetic media, laptop computers. This could occur in your hotel room, in an airport, in a conference room, or in any other situation where the opportunity presents itself and your materials are vulnerable.
- **Electronic Interception:** Use of devices to electronically monitor an individual's use of modern telecommunications, office, hotel, portable telephones, faxes and computers.
- **Technical Eavesdropping:** Use of audio and visual devices, usually concealed in hotel rooms, restaurants, offices, cars, airplanes.

Be Aware of the Following Recruitment Cycle Frequently Used by Foreign Intelligence Services

Spotting ⇨ Assessment ⇨ Recruitment ⇨ Handling ⇨ Termination

- **Spotting:** Stage of identifying potential intelligence targets.
- **Assessment:** Learning as much as possible about the targeted individual.
- **Recruitment:** Choosing a method of recruiting the individual for information, usually using a motivator of some kind such as money, ideology, compromise, or ego.
- **Handling:** Recruited target begins to provide the intelligence service with classified/sensitive information.
- **Termination:** When espionage activities come to an end.

What else should I be aware of while traveling?

Here are some additional tips to help you stay safe and keep your information secure while traveling.

- Maintain control of sensitive documents or equipment at all times.
- Do not leave sensitive materials in hotel rooms or hotel safes.
- Limit sensitive discussions.
- If taking an unclassified computer to a foreign country, ensure there is no sensitive, classified, or proprietary information stored on the computer.
- Upon your return, computers must be inspected prior to returning on site.

Contact your local CIO for additional information and literature about elicitation and the recruitment cycle, and to learn how you can protect yourself and the information you carry while on foreign travel.

Who do I contact regarding counterintelligence requirements for foreign travel?

As mentioned above, employees and contractors are required to receive pre- and post-briefings if travelling to a sensitive foreign country. Contact your local counterintelligence officer or the Office of Counterintelligence at (202) 586-1247.for further information about foreign travel briefings.