



Counterintelligence Threat to Academic and Scientific Travelers

When you travel overseas in an academic or scientific capacity you are subject to intelligence collection by foreign intelligence and security services (FISS). FISS are responsible for identifying individuals who can give them access to people and information in the US as well as acquiring information that will advance indigenous research and development. Traveling academic and scientific delegations afford FISS an ideal opportunity to gather information on US subject matter experts.

- You are known to government institutions before travel because of your visa
- FISS are in a permissive environment when operating in their home country and can scrutinize you either by design or chance using one of many justifications:
 - Fitting a criminal, or other profile
 - Participating in “black-market” activity
 - Possessing a banned or strictly controlled material
 - Associating with persons whom the government views as dissidents
 - Having language fluency, declared relatives, or organizational affiliations in the country you are visiting

FISS intelligence collection operations are usually unobtrusive, non-threatening and conducted without your knowledge. Although less common, some FISS use more aggressive or provocative measures meant to intimidate or “test” your reaction. Intelligence collection methods used by FISS include:

- *Elicitation* – a ploy whereby FISS use seemingly normal conversation to extract information about your work and associates
 - Elicitation is the most noticeable form of intelligence collection
 - It can be difficult to identify and is easy to deny

Examples of Elicitation

Direct questioning
Normal curiosity
False statements

Flattery
Word repetition
Opposing stand

Naiveté
Leading questions
Disputing accuracy

UNCLASSIFIED

- Exhaustion—scheduling a lengthy or extensive itinerary of events and activities designed to tire visitors and make them pliable.
 - Drivers or guides frequently accompany visitors and engage in elicitation
- Eavesdropping – listening in on conversations for information
 - Usually in social settings (bars, restaurants, or public transportation, etc.) where talking “shop” often occurs
- Technical Eavesdropping – use of audio/visual devices (often concealed) installed in public and private facilities, especially hotels and restaurants
- Surreptitious Entry—entry into your hotel room (often hotel assisted), accommodation or office to access documents or electronic information
- Electronic Interception – Fax, Telex, cell phones, and the internet are vulnerable to monitoring due to government control of telecom infrastructure
- Physical Surveillance –monitoring of your movements and activities

Common sense and basic CI awareness can effectively protect you against FISS attempts to collect sensitive information. Things you can do include:

- Do not leave sensitive materials in hotel rooms or safes
- Do not use computers or faxes at hotels or business centers for sensitive material
- Do not discuss information with someone who does not have a reason to know it
- Keep your personal computer as carry-on baggage
- Do not leave cell phones or portable electronics unattended
- Do not attempt to locate listening devices
- Do not attempt to evade physical surveillance
- Report CI incidents when you return

In addition, there are several things you can do to successfully counter elicitation:

- Prepare talking points ahead of time that do not disclose sensitive information
- Do not engage in conversation alone
- Redirect the conversation
- Excuse yourself from the conversation
- Reply to a question with a question
- Provide vague or hypothetical responses
- Provide historical, publicly known information
- Change the topic
- Feign ignorance
- Ask “Why?”

If you observe any activity that seems to be out of character with the purpose of a foreign visit, please contact the FBI Cincinnati Field Office at (513) 421-4310.

<http://www.uc.edu/infosec/export/>

UNCLASSIFIED