

CONSCIENTIOUSNESS OR CARELESSNESS?

Remember, whether the person, the information, or both are traveling overseas, information electronically transmitted over wires or airwaves is vulnerable to interception and exploitation by foreign intelligence services. Many countries have sophisticated eavesdropping/intercept technology and are capable of collecting information we want to protect, especially overseas. Telephone and fax transmissions are targeted by numerous foreign intelligence services and/or other foreign entities that are supported by their governments. Voice, fax, cellular, data and video signals can be easily intercepted.

At the most basic level, it is the conscientiousness or carelessness of the individual person that determines whether or not our information is protected from unauthorized disclosure.

The DSS Field Counterintelligence Specialist servicing this area is:

This publication has been produced by the Defense Security Service for use by US DoD Contractors and US Government Agencies as part of their security programs.

Questions and requests to further distribute this publication should be addressed to the Defense Security Service Public Affairs Office.

SECURITY COUNTERMEASURES

Some common sense security countermeasures should include:

- Don't publicize travel plans and limit sharing of this information to people who need to know
- Pre-travel security briefings
- Maintain control of sensitive information/documents and media/equipment. Don't pack these types of articles in checked baggage (keep as hand carry/carry-on). Don't leave these unattended in hotel rooms or stored in hotel safes.
- Keep hotel room doors closed/locked. Note how the room looks when you go out.
- Limit sensitive discussions. Generally speaking, public areas are rarely suitable for discussion of sensitive information.
- Don't use computer or fax equipment at foreign hotels or business centers for sensitive matters.
- Ignore or deflect intrusive or suspect inquiries or conversations about professional or personal matters.
- Keep unwanted (no longer needed) sensitive material until it can be disposed of securely. (Burn or shred paper; cut floppy disks, as appropriate).

**Bottom line:
be Alert... be Aware... Report
suspicious occurrences!**

Public Affairs release #050922-01

Foreign Travel-Related Vulnerability



This product created by the
Defense Security Service (DSS)
Counterintelligence Office

OVERSEAS TRAVEL

Overseas travel increases the risk of being targeted by foreign intelligence activities. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you and their actions are not restricted when they are operating within their own countries.

Information Age spying includes:

- wired hotel rooms
- intercepts of fax and email transmissions
- recording of telephone calls/conversations
- unauthorized access and downloading, including outright theft of hardware and software
- break-ins and/or searches of hotel rooms, briefcases, luggage, etc.
- bugged airline cabins
- substitution of flight attendants by spies/information collectors.



FAVORITE TACTICS

The overseas traveler and the information in their possession are most vulnerable when on the move. Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside the hotel room) may be recorded. These recorded observations can then be analyzed for personal vulnerabilities (useful for targeting and possible recruitment approaches) and/or useful information (collections).

A favored tactic for industrial spies is to attend trade show/conference type events. This environment allows them to ask a lot of questions, including questions that might seem more suspect in a different type environment. One estimate reflected that one in fifty people attending such events were there specifically to gather intelligence.



COMPUTER SECURITY

Another area of concern while traveling is computer security. Foreign Intelligence Services are not usually fortunate enough to have information simply dropped into their hands. They rely on tactics such as stealing laptops. These portable systems may contain access capabilities that serve as doorways to additional information and systems. A recent survey of U.S. corporate security directors disclosed that 150 of 521 reports reflected thefts of laptops during the previous 12 months. Additionally, 62 percent reported computer security breaches despite increased use of firewalls, encryption and digital identification. Bounties are sometimes put on laptops and are targeted even if the particular person is not specifically targeted.

In addition to theft, travelers have reported unauthorized access, attempted access, damage and evidence of surreptitious entry of their portable electronic devices.

Effective countermeasures to the aforementioned vulnerabilities include but are not limited to the following:

- Refrain from bringing portable electronic devices unless it's mission critical
- Use of removable hard drives
- Maintain personal cognizance of portable electronic devices
- Data on portable electronic devices should contain only what is needed for the purpose of your travel