Inadvertent Leaks versus Conscious Disregard

While traveling overseas, any information electronically transmitted over wires or airwaves is vulnerable to foreign intelligence services' interception and exploitation. Suspicious entities can easily intercept voice, fax, cellular, data, and video signals.

Many countries have sophisticated eavesdropping/intercept technology and are capable of collecting information we want to protect, especially overseas. Numerous foreign intelligence services target telephone and fax transmissions.

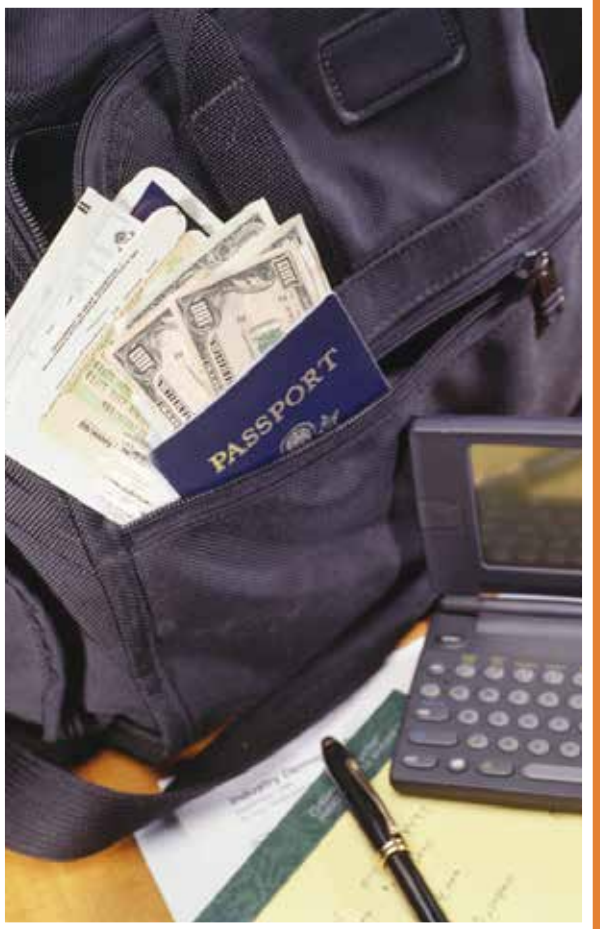
Your diligence determines whether or not our sensitive information is protected from unauthorized disclosure.

Security Countermeasures

- Do not publicize travel plans and limit sharing of this information to people who need to know
- Do not post pictures or mention you are on travel on social media until your return
- Attend pre-travel security briefings
- Maintain control of sensitive information, media, and equipment. Pack them in your carry-on luggage and maintain control of them at all times. Do not leave them unattended in hotel rooms or stored in hotel safes
- Keep hotel room doors locked. Note how the room looks when you leave compared to when you return
- Limit sensitive discussions; public areas are rarely suitable for discussion of sensitive information
- Do not use computer or fax equipment at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspicious inquiries or conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely
- Attend post-travel debriefing and report any and all suspicious activity

Be Alert! Be Aware!

Report suspicious activity to your local security official.



Foreign Travel Vulnerability

Defense Security Service
Counterintelligence Directorate
www.dss.mil

FOREIGN TRAVEL VULNERABILITY

Foreign Travel

You can be the target of a foreign intelligence or security service at any time and in any place; however, the risk is greater when you travel overseas.

When overseas, the foreign intelligence services have better access to you, and their actions are not restricted within their own country's borders.

Collection Techniques to be Wary of

- Bugged hotel rooms or airline cabins (including video surveillance)
- Intercepts of fax and email transmissions
- Recording of telephone calls/conversations
- Unauthorized access and downloading, including outright theft of hardware and software
- Installation of malicious software on computers or personal electronic devices
- Intrusions into or searches of hotel rooms, briefcases, luggage, etc.
- Recruitment or substitution of flight attendants
- Individuals appearing to try and eaves-drop on your conversations
- Individuals attempting to read your computer screen or documents over your shoulder

Preferred Tactics

Overseas travelers are most vulnerable during transit. Travelers should be wary of extensive questioning from airport security, luggage searches, and downloading of information from computers and personal electronic devices.

Travelers should maintain heightened awareness once they reach their destination. Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside their hotel room) may be monitored and recorded.

Entities can analyze their recorded observations for collecting information or exploiting personal vulnerabilities. This information is useful for future targeting and recruitment approaches.

Another favored tactic for industrial spies is to attend trade shows and conferences. This environment allows them to ask questions, including questions that might seem more suspect in a different environment.

Computer Security

Cleared contractors provide critical research and support to programs giving the United States an economic, technological, and military advantage.

In a world where reliance on technology continues to grow, foreign entities have increased the targeting of electronic devices such as laptops and cell phones.

Travelers should report theft, unauthorized or attempted access, damage, and evidence of surreptitious entry of their portable electronics.

The following countermeasures can decrease or prevent the loss of sensitive information:

- Leave unneeded electronic devices at home
- Use designated travel laptops that contain no sensitive or exploitable information
- Use temporary email addresses not associated with your company
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Encrypt data, hard drives, and storage devices whenever possible
- Use complex passwords
- Enable login credentials on laptops and devices