Defense Nuclear Security
Lessons Learned Center
Sharing Experiences to Ensure National Security
NNSA National Nuclear Security Administration

February 2008

Be Security Smart!

The following security tips are an excerpt from a counterintelligence awareness booklet prepared by the Office of the National Counterintelligence Executive (ONCIX). More security awareness tips from ONCIX can be found at: http://www.ncix.gov/publications/booklets_brochures/booklet_beAlert/Be_alert_2003_200.pdf

You Are the Target!

US citizens traveling abroad continue to be the target of foreign intelligence collection activities. Many foreign governments and foreign businesses place a high priority on acquiring US Government and private industry protected information (classified, sensitive, and proprietary). Although the Cold War has ended, the risk of becoming an intelligence target has increased. The threat you face as an official US Government traveler is real. This Security Smart describes several aspects of the nature of the foreign intelligence collection threat. Future Security Smarts will provide descriptions of additional potential threats, present some basic steps you can take to mitigate the threat, and describe the actions you should take to report suspicious incidents.

Eavesdropping

As we all know, eavesdropping is listening to other people's conversations without their knowledge to gather information. Eavesdropping activities can range from the strategic positioning of an unobtrusive bystander, to the use of concealed sophisticated audio and visual devices.

- Frequently employed in social settings where attendees feel secure and are more likely to talk about themselves and their work.
- Frequent venues include public and host-provided transportation, restaurants, bars, and meeting facility restrooms.
- Concealed devices are cost efficient, low risk, and can be used in conjunction with overt devices such as traffic and pedestrian-monitoring cameras.

Electronic Interception

Electronic interception is the legal or illegal seizure of electronic communications. This method is increasingly conducted against modern telecommunications systems and personal electronic devices, such as personal digital assistants (PDA).

- Foreign telecommunications carriers are particularly vulnerable because most are government controlled.
- Office, hotel, and portable telephones are key targets.
- Facsimile, telex, and e-mail can be electronically monitored.
- Many countries have the ability to intercept and possibly break commercially available encryptions.