

January 2009

Be Security Smart!

Technical Surveillance Countermeasures

The Technical Surveillance Countermeasures (TSCM) program is designed to detect, deter, isolate, and nullify technical surveillance penetrations and technical security hazards. TSCM technicians use several techniques and a variety of electronic and electrical equipment to detect illegal devices, more commonly known as "bugs," designed to listen to or transmit information.



Awareness

All employees should be aware of the threat of technical surveillance, which can come from an insider or outsider. Employees can take the following precautions to reduce the threat:

- Be alert to strange or unauthorized personnel performing maintenance in your area.
- Listen for strange occurrences when using your telephone, such as clicking noises, callers complaining about one line being busy most of the time, long delays in dial tones when you pick up the receiver, echoes in your phone during local calls, or telephone repairmen working on your telephones without your request.
- Be aware of your surroundings, especially changes to furniture, clocks, and office equipment.

Suspect Threat

If you suspect or become aware of a technical surveillance penetration, take the following steps:

- Stop all classified discussions while maintaining other normal activities in the area.
- Protect the area so that no one can remove the suspected device.
- Immediately report the incident to your security responsible line manager and the TSCM Team, but do so away from the area where you believe the threat to be.
 - ◊ Requests for TSCM services, which include technical or site-specific information, may be classified Secret/National Security Information and should be arranged by a secure means (in person, classified hard copy correspondence, or secure communications methods).
 - ◊ If reporting cannot be done by secure means, simply state that you need to talk to a member of the TSCM Team immediately.

If you are on travel to a foreign country and suspect that your equipment (e.g., laptop, PDA, government-issued cell phone) has been tampered with during your stay, contact the TSCM Team upon your return.