



CORPORATE ESPIONAGE

COUNTERINTELLIGENCE AND TECHNICAL COUNTERMEASURES
TECHNICAL SURVEILLANCE COUNTERMEASURES

Technical Surveillance Countermeasures (TSCM)

TSCM includes all countermeasures employed to prevent or detect the interception of sensitive, classified or private information. TSCM is typically an inspection by an experienced technician of a physical item or place (briefcase, automobile, office, home, boat, etc...). The purpose is to locate possible covert surveillance devices (bugs), technical security weakness and technical security hazards. A TSCM specialist can also evaluate for weaknesses of all locks, alarms and other systems of physical and electronic security or controls.

Vulnerability Analysis/Threat Assessment

A formal vulnerability analysis or threat assessment should be performed prior to any TSCM sweep. The TSCM specialist would visit the facility for several days and identify weaknesses with locks, doors, alarms, fence lines, video cameras, telephone systems, network and computer security. The end product for a vulnerability analysis is a written report addressing specific issues or concerns requiring attention.

It's strongly recommended to first have a careful vulnerability analysis or threat assessment completed before having any TSCM work done.

The primary purpose of a vulnerability analysis is to identify the following:

- Potential adversaries
- High risk and sensitive information
- Method(s) of potential attack
- Location(s) of potential attack
- Vulnerability based on timelines and events
- Areas of highest vulnerability

Multi Level Detection Plan

An evaluation involving minimal equipment of a sensitive facility, to determine physical security measures required to protect against technical penetration or unaided audio leakage.

In Place Monitoring System (IPMS) is used during this inspection. This is the simplest and lowest level type of legitimate TSCM sweep. It consists of monitoring a given office or location while an event or meeting is in progress. IPMS assume that the facilities are secure and that the only threat is from meeting attendees possessing an electronic surveillance device for transmitting room audio.

Comprehensive TSCM Survey/Sweep

A detailed electronic, visual and physical examination of a sensitive facility by TSCM personnel to ascertain that the area is free of technical penetrations and to detect technical security hazards and weaknesses.

This inspection requires that every wire in a given area is checked for covert listening or video devices. Sequentially, the survey begins with a RF search, followed by a wire and conductor check, a complete physical search and concludes with an inspection of the telephone room and related instruments.

The amount of formal TSCM training needed to do this type of a sweep is extensive (500 hours minimum), plus an expert level of knowledge in security, electronics, surveillance equipment, surveillance equipment installation techniques, communications, and computer science. Most of the best training and experience comes from government (state or federal) agencies for this type of work. A Comprehensive TSCM Survey/Sweep requires the extensive use of highly technical and sensitive equipment.

This type of inspection is commonly performed at military facilities, embassies, defense contractors, DOE facilities, Corporate Boardrooms etc... This survey will locate not only transmitters that are operating, but also microphones, recorders and any surveillance equipment in place that could be remotely operated. In addition this survey may also detect the existence or evidence of historic electronic surveillance equipment.

PHONE: 212 860 2800
PHONE: 212.260.2534
FAX: 212.260.2535

1617 3RD AVENUE #286150
NEW YORK, NY 10128
WWW.EAGLEGUARDSECURITY.COM
INFO@EAGLEGUARDSECURITY.COM