INTRODUCTION TO TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)

The following points are of importance with a Risk Assessment and Evaluation by means of physical Inspections:

MINIATURE TRANSMITTERS

The areas investigated are situated in open line of sight to numerous other offices, boardrooms, open areas and roads all of which can facilitate hostile eavesdropping attempts by miniature radio transmitters.

TYPICAL FEATURES OF MINIATURE RADIO TRANSMITTERS

- Transmitting Range – approximately 500 meters;
- Approximately the size of a Matchbox;
- Can be adapted/made smaller, e.g. to fit into a pen or ashtray, where the Transmitting Range will typically be reduced to 30 meters;
- Such Transmitters may easily and quickly be installed and removed (even by a non-technical person)

PLEASE NOTE:

- Transmitting Range of a 'few kilometers" for this type of device, often quoted in the press, cannot be achieved without using extremely sophisticated and expensive equipment often only obtainable from overseas markets.
- The Transmitting Ranges indicated above are only examples of typical values. Actual distance will depend on factors such as the placing of the receiver, type of receiving antenna, actual transmitter power, etc.
- Transmitter Power is dependent upon physical size of the **transmitter, battery life and transmitter output power.**

In Conclusion, the Risk Factors concerning the Deployment of Listening Devices should be considered as:

- Miniature Radio Transmitter - **High Risk**
- Line Tape Recorder - **High Risk**

TELEPHONES

The insertion of "taps" or eavesdropping devices on telephone lines outside control areas (client's premises), is always a threat incurring difficulty in **detection**. The use of telephones, particularly not having "fail safe" encryption devices (scramblers), should always be considered vulnerable. Cellular telephones believed much safer to use, are overall more difficult to monitor. However, they are vulnerable to monitoring with the assistance of network providers and also by expensive, sophisticated equipment obtainable from overseas markets or, in extreme cases, the placing of a "bug" within the cell phone. Mobile device malware (malicious code) has increased exponentially over the past few years. Anyone can install eavesdropping software on a smart phone, as long as they have access to the phone even for a few minutes. This can result in them gaining access to all your private data and even listen in on actual calls.

PARASITIC DEVICES

There are two main types of parasitic devices in the market, currently used by criminal elements:

1. RF Radiating Devices:

These devices use a RF carrier wave to transfer information to a remote receiver unit. By using wide-band scanning receivers, one is able to intercept or detect the radiated RF waves and determine its origin.

2. Parasitic Recording Devices:

As recording devices do not radiate recognisable signals, detection methods vary from that of radiating devices. The best method of ensuring parasite free lines is to physically disconnect both ends of the line and test each line individually for series and parallel parasitic devices. Unfortunately, this method is time-consuming, however currently proven “fail-safe”, with these techniques conducted separately, from RF counter-measures tests.