

## **TSCM Listening Post - The Sweep**

An article by Peter J Lynch – Lynch Investigations & Countermeasures Pty Ltd

### **TSCM - Technical Surveillance Counter Measure ECM - Electronic Counter Measure**

It is a good idea to have a contractual agreement with your client for the TSCM Debugging Investigation Services your business supplies. It is recommended to determine the scope of the TSCM Debugging Investigation so that you can give a reasonable quote for your TSCM Debugging Investigation Services.

Some clients may want several small business offices swept or a large residential building. The building design, structure type & the objects within the building will need further inspection. You will need to ascertain the contents within the building to estimate your best quotation for the TSCM Debugging Investigation Service that your business provides. Computers, telephone systems, electrical fittings & furnishings are items that will need careful consideration.

Some clients may just want the telephone lines vetted to make sure that they are clean while other clients may need a full TSCM Debugging Investigation Service.



Thinking about how a person would go about the espionage & what would be the easiest & most effective methods they would use. What kind of information does the bugger wish to obtain? How much is the information sought after & worth to your client? How much time does a person need to expend to obtain the information?

After reviewing the businesses security it may be considered to install ECM equipment, considering all areas to be covered initially with a sweep, can clear the area of any suspicion. ECM equipment can disable, mask or jam or otherwise render ineffective any surveillance equipment already in place.

The next step is to decide whether the sweep should be a covert sweep or you may decide that it doesn't matter if the bugger knows that their device is being searched for. Disinformation may be supplied by the client to the bugger if the client knows that they are being monitored. Alternatively the bugger may just wait until they know that the sweep is finished and plant another device.

There may be a critical time limit prior to a corporate meeting that commences in an hour, where a director is cautious about the possibility of a compromised room; here a covert operation may become almost impossible.

In many instances it is usually more appropriate to run a covert sweep when staff are away from the building, starting earlier in the evening and working through the night & into the early morning hours as required and where possible.

The sweep team member number would be considerably less for a residential sweep than the number and quality of TSCM Debugging Investigation experts required for a sweep at an embassy or a defence force communications room.

It is useful to have a floor plan of the building with each team member assigned to a different task. Each sweep team member can then follow an assigned task to reduce the amount of confusion & lost time. If prior photos of the building are available that the sweep team may have taken from a previous sweep, these are useful also that will allow any change in the sweep area to be observed in respect of new objects, items and changes to the area where the TSCM Debugging Investigation is to occur.

Some sweepers will check for video transmissions before entering the building on the common transmission bands. This may prevent a compromise before the sweep team enters the building. It may be possible that video surveillance from inside of the building is remotely controlled & compromise is difficult in being avoided.

A covert sweep team may use a van with cleaning services in advertising on the outside of the van. Many operatives will employ disguises like cleaning services with trolleys. The cleaning equipment is used to hide the TSCM equipment while the operatives enter the

building or business to be swept. Once inside the area, conversation about cleaning can disguise the team with code or hand signals used to communicate anything about the sweep.

When the sweep team is inside of the building each team member can go about their allocated task. One group will check all likely places bugs can be concealed, on the walls & floors, removal of the AC outlet covers, TV outlet & coaxial cables, looking for unusual connected wires and devices or a disturbance within the building structure fittings & objects within.

It is also a good idea to search light fixtures, smoke detectors, loose ceiling panels, all electrical appliances, cupboards & plants in the building. A bug can be hidden anywhere in a room, in the hollow of a book, lamps, TVs, clocks, computers or radios.

No matter how small the chances are of finding a bug in an unusual location, all possibilities should be investigated. The phone system should be thoroughly checked by unscrewing the covers from the phone. An experienced TSCM sweeper will know what should be in place. The telephones microphone and speaker areas are good places to inspect for any additional or recently connected wires.

A TSCM sweep team can apply their seals to the electrical appliances casings. Upon opening the casing of an appliance and putting it back together a check seal can be placed discretely between the appliance covers to aid in detecting future tampering of the appliance.

It is also a good idea to check the operating voltage of the telephone & to determine any low voltage values than normal, for the off hook telephone position. There may be a parasitic device powering its circuit from the telephone power source. As well as checking the telephone lines, check all telephone plugs and fittings carefully. Ensure that the computer, fax & modem are all in order.

It is not a good idea upon finding a bug to pack up the TSCM equipment & think that the sweep is completed. We have heard of commercial offices with many bugs planted where the bugger has planted a bug in an obvious location with the bugger

thinking that after the TSCM sweep team was to find the first device, all further search efforts would be terminated.

A physical inspection is recommended for hard wired systems where possible. A bugger will nearly always prefer to use pre-existing wiring to get the signal to the outside world, where it can be taped or transmitted. Common areas used for bugging are alarm wiring, phone lines, fax & modem lines, antennas & telephone distribution systems. Phone systems & alarm sensors should be inspected for any signs of tampering.

An existing television cable can be used to send a signal from a hidden video camera in a room by modulating or mixing the signal that travels along the cable. The bugger can tap into an outlet served by the same source (antennae or cable feed) & tune in their signal. A portable TV can be used to connect to such a signal tuning above & below all TV channels by tuning through VHF & UHF frequencies.

Only experience can tell you how much time to spend on a physical inspection before moving onto the RF sweeping & telephone analysis.

A conference room may be physically searched in a short period of time where an office room with lots of equipment & furnishings can take all night. The size of the TSCM sweep will ultimately determine the time management requirement for your TSCM Debugging Investigation.

[Visit the PJJ Online Store for the best priced investigative equipment](#)

All the best of luck with your TSCM sweep

PJJ.

Web Site: [www.pjlinvestigations.com.au](http://www.pjlinvestigations.com.au)

***Disclaimer*** This information is given as a means of providing an introduction to TSCM Debugging Investigations. It is not provided with the intention of giving a comprehensive understanding of the way in which TSCM Debugging Investigations occur. Such an understanding should be based on technical manuals which relate to TSCM Debugging Investigation Services & on advice of those qualified to advise on such matters.