

TSCM Listening Post – TSCM Threat Level

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

Low level threats require search by electronic means for video devices, audio transmitting devices, carrier current devices and a visual inspection of telephone lines including the main distribution frame (MDF), intermediate distribution frame (IDF), Krone blocks and the external junction boxes attached to the building and throughout the structure. A limited physical and visual inspection is performed that is quick and basic that can locate various types of typical low level threats.

The low level threat includes private & personal information usually involving or relating to domestic disputes, targeted radio scanning, monitoring, the interception of cordless telephone conversations and other assisted surveillance activities.

Medium level threats require search by electronic means for audio transmitting devices, video transmitting devices, hard wired audio and video devices, carrier current devices and physical telephone analysis from the exterior junction box attached to the building and all distribution frames and Krone blocks. In addition an extensive physical and visual search is conducted of the premises including electrical outlets, switches and other items considered to be a possible threat.

The medium level threat includes confidential and sensitive information relating to high profile sales and marketing, lawyers, disgruntled employees, issues surrounding labour unions, information relating to criminal harassment & stalking, invasion of privacy issues and investigative monitoring.

High level threats require years of extensive and ongoing training with an investment upwards of \$500,000 in equipment. TSCM Debugging Investigation Services at this level are provided by former intelligence agents. This TSCM threat level will require the detection of all forms

of equipment including ultra high end eavesdropping equipment placed by governments for espionage of other governments.

The high level threat requires an agent's full dedication to countermeasures and TSCM knowledge. The majority of work at this level is from professionals that work for either military intelligence or federal government. There are very few TSCM agents in the private sector market at this level of counter-intelligence. Security departments of high tech corporations are sometimes able to provide this level TSCM Debugging Investigative Service at upwards of \$5,000.

Through consultation with your TSCM service provider you can determine the level of threat or whether a compromise may in fact exist. You should remember that an effective and detailed TSCM Debugging Investigation requires many years of specialised technical training, certification & experience. An up to date list of the TSCM specialist's equipment and resources is needed. It is extremely important to make your choice of TSCM services in this regard.

There are some companies that charge cheap prices for TSCM Debugging Investigation Services and are ineffective because they have no experience or training. These service providers are willing to charge a fraction of the cost of what a professional TSCM Debugging Investigation is worth, or on the other extreme excessive rates for a low grade TSCM Debugging Investigation Service. These operators will provide you with a false sense of technical security. A quality TSCM Debugging Investigation will be very time consuming and tedious, requiring an extremely high level of knowledge and experience.

At the high level threat, the protection of classified and restricted information relating to such issues as national security, embassy, military, government and law enforcement related functions are all in need of careful decision making regarding the TSCM Debugging Investigation and TSCM Debugging Investigation Service provider to be contracted to provide extremely high quality TSCM Debugging Investigative Services.

Like any professional service you should research and educate yourself before contracting a TSCM firm to take on an extremely important task for your concerns.

All the best of luck with analysing your TSCM threat and engaging your professional TSCM agent.

PJL.

Web Site: 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.