## ACS – TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) "DEBUGGING"

The threat of Corporate Espionage remains a reality. A regular programme of Technical Surveillance Countermeasures (TSCM) "debugging" is recommended towards ensuring the protection of Company Intellectual Property (IP) and Communication Security.



Intellectual Property is more than just an idea or a concept

— it relates to assets that may be integral to the core services
and overall long-term viability of a Business.

Companies of all sizes are at risk of having their unique ideas, products or services infringed upon, even if they are on the other side of the world, making Intellectual Property Protection more important than ever.



The key focus of our specialised service delivery is the Protection of Intellectual Property and comprises of four pillars. The first pillar focuses on Technical Surveillance Counter Measures (TSCM) "Debugging" and the detection of malicious eavesdropping devices. During a TSCM "Debugging" investigation, weaknesses in technical and communications security are identified, and solutions offered.

A main contributing factor to Corporate Espionage as well as the use of listening and video devices is the increasing sophistication, durability, and ready availability of items on the market. "Bugging" devices can be readily bought over the counter and through popular online retailers, and the devices are smaller and capable of being on for longer periods to capture information. This makes the corporate spy's job easier and highlights once again the importance of implementing a regular programme of TSCM "Debugging" as a pro-active security measure.



ACS provides all-encompassing and comprehensive TSCM "Debugging" Investigations using the most modern and technologically advanced equipment available in South Africa.

Contact: Riaan Bellingan +27(0)82 491 5086 | riaan@acsolutions.co.za www.acsolutions.co.za