ComSec – Professional TSCM Service Provider

Technical Surveillance Countermeasures (TSCM) Equipment

For professional TSCM / Cyber TSCM surveys to be effective, the TSCM specialist must be sufficiently trained and properly equipped. Eavesdroppers utilize a variety of devices and spying tactics to exploit vulnerabilities in your security protocols with the intent of accessing and utilizing your valuable information.

A professional TSCM / Cyber TSCM provider ensures the knowledge and skills of its specialists and the eavesdropping detection equipment utilized are capable of detecting spying devices and exposing eavesdropping tactics. Professional TSCM service providers are aware that electronic eavesdropping devices and tactics are continually evolving. In order to provide thorough and effective TSCM services, the professional TSCM service provider must ensure their specialists, equipment and processes continually evolve to address the emerging threats.

The ComSec LLC Advantage:

- ComSec's TSCM specialists have extensive knowledge of TSCM fundamentals, spying tactics and eavesdropping devices.
- ComSec's TSCM specialists receive professional training in the application and proper use of ComSec's TSCM equipment.
- ComSec utilizes proprietary operational methods and techniques in providing professional TSCM / Cyber TSCM services.
- ComSec's equipment resources include a wide range of sophisticated (classified and unclassified) commercially available, Cyber TSCM and telecommunication test and measurement equipment.
- All TSCM/ Cyber TSCM equipment is regularly qualified, serviced and maintained to the highest technical standards available.
- ComSec's eavesdropping detection equipment is constantly upgraded to meet new and emerging technical surveillance threats. This practice ensures that we are prepared and fully capable of handling all known threat levels as well as the continuous technological advancements with regards to covert Technical Surveillance Devices (TSD), Technical Security Hazards (TSH), espionage methods, techniques, compromises and the more common non-electronic methods of compromise.
- ComSec carefully analyzes each individual survey assignment and selects different combinations of equipment, inspection methods and techniques as required for both known and developing threat levels.

ComSec – Professional TSCM Service Provider

Technical Surveillance Countermeasures (TSCM) Equipment

Commercial - Unclassified TSCM Equipment

ComSec LLC utilizes the following commercial, unclassified TSCM equipment for its professional, commercial eavesdropping detection services.

REI OSCOR Green (24 GHz) TSCM Spectrum Analyzer - The OSCOR Green is designed for commercial applications to detect illicit eavesdropping signals, perform site surveys for communication systems, conduct radio frequency (RF) emissions analysis, and investigate misuse of the RF spectrum. OSCOR Green scans 24GHz in one (1) second ensuring spectrum activity is captured, which is the equivalent of capturing 2,000,000 data points per second.

KESTREL TSCM PRO -The Kestrel TSCM Pro Equipment Software Application Interfaces, Wireless Network Analysis Technology, GPS Mapping and Logging Tools, RF Spectrum (Real Time and Post Analysis) Software, Global Frequency Database and a Proprietary Telephone, Video Conferencing, Voice, Data and Wireless Systems Engineering Reference Database.

Kestrel TSCM Professional Software - Signal Intelligence Support System (SISS) (BB60A-6.0 GHz) / (12.4 GHz) Dual / Multiple Receiver with Remote Surveillance and Monitoring Capability, Differential Signal Analysis (DSA) and advanced Threat Level Programming (TLP).

REI - ORION 2.4GHz Non-Linear Junction Detector (NLJD) - A Non-Linear Junction Detector detects the presence of electronics, regardless of whether the electronic target is radiating, hard wired, or even turned off. The ORION 2.4 locates hidden electronics in walls, floors, ceilings, fixtures, furniture, or containers. The NEW ORION 2.4 transmits at 2.4GHz frequency for detecting small electronics such as SIM cards and cell phones.

BUCLET-2 Handheld Non-Linear Junction Detector (NLJD) 2.4 GHz Technology.

FLIR E8 & E60 Thermal Imaging Camera, 320 x 240 IR-MSX Resolution.

REI CPM-700 Counter Surveillance Broadband Receiver - The CPM-700 is a broadband receiver designed to detect and locate all major types of electronic surveillance devices including room, phone, body bugs, video transmitters, and tape recorders. Monitor Probe with VLF (150 MHz) / Infrared (IR) / RF (12 GHz) / Magnetic Leakage / Audio Acoustical Leakage / High Gain Audio Amplifier).

REI TALAN DPA 7000 Telephone and Line Analyzer - The TALAN incorporates several types of telephone line tests including common tests such as voltage, current, resistance, and capacitance tests, as well as NLJD, FDR Frequency Domain Reflectometry, and Digital Demodulation technology into a single piece of equipment. Voice-over Internet Protocol (VoIP) phone systems present a new form of security risk to communications. With new enhancements built into the TALAN software interface, users can now test internet protocol (IP) packet traffic on VoIP phones and systems. VoIP data collected by the TALAN software includes Source and Destination Mac Addresses; header type; statistics – total packets; packet rate; peak rate and run time.

ComSec – Professional TSCM Service Provider

Technical Surveillance Countermeasures (TSCM) Equipment

CELLEBRITE Physical Analyzer - The UFED Physical Analyzer is the most powerful and technologically advanced mobile forensic application available. It exposes every segment of a device's memory data and provides in-depth decoding, analysis and reporting methods. Features include: Malware Detection – On-demand searches for viruses, spyware, Trojans and other malicious payloads in files, Project Analytics – View statistics on communications and identifying relationship strengths Rich Set of Data – Includes calendar, call logs, contacts, SMS, MMS, chats, applications etc. The advanced application for decoding, analysis and reporting.

FLUKE One Touch Network Analyzer - VoIP: inline VoIP call monitoring and comprehensive logging simplifies troubleshooting of desktop VoIP problems in real-time without taps or switch mirror ports. Capture: wired, Wi-Fi, VoIP and AutoTest packet capture streamlines collaboration and escalation of the most complex issues.

FLUKE AirCheck Wireless WiFi Analyzer - Detect and locate 802.11ac APs; validate connectivity to 802.11ac infrastructure, One-button AutoTest quickly provides a pass/fail indication of the wireless environment and identifies common problems, See wireless network utilization by channel and quickly determine if it is 802.11 traffic or non-802.11 interference, Quickly identify and locate wireless access points whether authorized or rogue, etc.

*Classified-ITAR Controlled-Restricted TSCM Equipment

*Available to US Government and US Military Clients Only.

ComSec owns and operates additional TSCM and Cyber TSCM equipment and proprietary software programs that are not listed above for a variety of security related reasons. These additional equipment resources are utilized where the threat level of the target area requires extraordinary OPSEC and additional inspection methods to be utilized.

When selecting a TSCM / Cyber TSCM service provider, utilizing a professional TSCM company with sufficiently trained specialists, the appropriate TSCM equipment and an extensive knowledge of current spying devices, threats and effective detection methods is the only choice. Contact ComSec LLC today for professional TSCM / Cyber TSCM services.

Global Counterespionage Specialists

Certified Counterespionage Information Security Management - CCISM

Licensed, Insured and Certified TSCM Service Provider | USA Nationwide | Worldwide Services