ComSec LLC TSCM / Cyber TSCM Services

TSCM is a highly specialized field. Clients who contact us are often unfamiliar with the terms used and/or the purpose of certain types of inspections we perform. This document was designed as a resource for our clients to learn more about TSCM / Cyber TSCM and ComSec LLC's services. If you have any additional questions after reading this document, please call us at (800) 615-0392 to discuss.

What Is Electronic Eavesdropping?

Electronic eavesdropping is electronically intercepting conversations, or other communications, without the knowledge or consent of at least one of the participants. Electronic eavesdropping is an old science, but the devices used now are anything but old school. Eavesdropping devices are now much smaller and more technologically advanced than ever. Modern eavesdropping devices capture audio, video and/or data remotely, and can be activated remotely. Current technologies can also utilize devices and networks that interface with cyberspace to eavesdrop or collect data. Electronic eavesdropping is easier and more effective than ever!

How Is Electronic Eavesdropping Accomplished?

Electronic eavesdropping can be accomplished with radio frequency transmitters (bugs), wire taps, IT network cabling, AC power lines, DC power lines, land-line telephones and faxes, drop-in recording devices, laser microphone, etc. Wireless communications, such as cell phones, and wireless data communications via Wi-Fi, BlueTooth or cellular networks can also be used for eavesdropping. For more information about the types of eavesdropping devices and their uses, visit our Spy Gadgets page.

What Is the Objective of a Technical Surveillance Countermeasures (TSCM) Service?

The objective is to determine if there is evidence of any technical surveillance devices or technical security hazards within the client's area(s) of concern. If they are present, the best course of action can be determined.

"Area(s) of concern" means the area(s)/room(s) for which ComSec LLC is contracted to provide TSCM / Cyber TSCM Services.

What Is TSCM?

Technical Surveillance Countermeasures (TSCM) is the process of "Sweeping A Room" to locate, eavesdropping devices that are installed in, or are present within, a building, room(s), vehicle(s), boat(s) or aircraft. This technique includes detecting body-worn transmitters or device-wired microphones. It also includes detecting devices located outside of the area of concern that are used to eavesdrop within the area of concern, such as laser microphones.

What Is Cyber TSCM?

Cyber TSCM involves detection of devices that access information on or from modern electronic devices (e.g. cellular phones, BlueTooth devices, computers, etc.) Cyber TSCM also includes detection of software, spyware/malware and other threats posed by modern electronic devices that operate within, or interface with, cyberspace. During your Cyber TSCM service, we also detect illicit eavesdropping devices that use the Wi-Fi or the cellular network to capture data, such as IMSI catchers or GSM devices.

ComSec LLC's Services Include Both TSCM and Cyber TSCM!

Rev. 03/11/2020

What Types of Inspections Are Included in ComSec's TSCM/Cyber TSCM Service?

ComSec LLC's Full Scope TSCM / Cyber TSCM Service Includes the Following Inspections:

Technical Threat Analysis (TTA):

This analysis includes a review of changes in your environment, your suspicions concerning eavesdropping in the area(s) of concern, identification of potential eavesdroppers, a discussion about the potential motives of the eavesdropper, potential weaknesses in your security posture, and related threat information. The information helps our team to better understand the service environment and any special considerations or precautions we must take.

Covert Video Analysis:

This analysis includes a full physical and electronic TSCM inspection for any surreptitious audio or optical technical surveillance devices in use in the area(s) of concern. This inspection identifies surreptitiously hidden wireless video threats. The examination is conducted using a Tri-Band wireless video cam scanner in the range of 900 MHz, 1.2 GHz, 2.4 GHz and 5.8 GHz.

Exterior / Interior Radio Frequency (RF) Mapping Spectrum Analysis:

This analysis includes recognition capabilities for digital, spread-spectrum and frequency-hopping transmitters in addition to standard analog devices. The analysis is completed on the exterior and interior of the area(s) of concern, and a comparison of the signals is made to identify potential threats. The examination is conducted using: 1) Predator RF Hunter 20 GHz Spectrum Analysis Kit in the range of 20 GHz, 2) An OSCOR GREEN Spectrum Analyzer (Enhanced Omni-Spectral Correlator) in the range of 10 kHz to 24 GHz, 3) Handheld Spectrum Analyzer HSA-Q1 in the range of a 0 to 13.4 GHz, and/or 4) KESTREL TSCM PRO Software - Spectrum Analyzer and Measuring Receiver (SAMR) in the range of 1Hz to 6 GHz.

Audio and Optical Device Physical and Electronic Analysis:

This inspection detects any surreptitious audio or optical technical surveillance devices in use in the area(s) of concern. The electronic analysis includes a carrier current analysis of AC outlets, telephone cable and other wiring to detect devices capable of transmitting communications.

Physical FLIR Thermal Survey:

This survey uses thermal analysis of electrical switches, outlets, computer jacks, thermostats, video cameras, suspended ceilings, etc. to identify evidence of installation, removal, modification or other overt signs of potential electronic eavesdropping.

Wireless Network – Cellular Network Analysis:

This analysis detects and monitors cellular attacks in real-time. It also identifies IMSI catchers, baseband processor attacks, rogue base stations and cellular jamming of the 2G, 3G and 4G/LTE networks. ComSec uses: 1) the ESD Overwatch system, which generates a continuously updated, national situation report by means of distributed detection and localization of a multitude of baseband attacks, as well as the manipulation of cellular signaling, 2) GSMK Cryptophone cellular baseband firewall sensors, and/or 3) other proprietary technology.
Essentially, the information generated by the Cellular Network Analysis arms decision makers with the tools to eliminate illegal use of IMSI catchers.
ComSec is the exclusive US commercial partner for the ESD Overwatch system.

ANDRE Counter Surveillance Broadband Receiver:

The ANDRE is a handheld broadband receiver that detects known, unknown, illegal, disruptive, or interfering transmissions. The ANDRE locates nearby RF, infrared, visible light, carrier current, and other types of transmitters. Quickly and discretely mitigate threats using the ANDRE Advanced Kit's wide range of accessories specifically designed to receive transmissions across a 1 kHz to 12 GHz frequency range.

What Types of Inspections Are Included in ComSec's TSCM/Cyber TSCM Service? (Continued)

Non-linear Junction Detection:

A non-linear junction detector (NLJD) detects hidden electronic devices in floors, walls, furniture or furnishing that may be radiating, those that are hard wired, and those in the area(s) of concern that are turned off. The examination is conducted using an ORION NLJD or the Handheld NLJD EDD-24T in the range of 2.4 GHz.

LED Refraction:

This inspection identifies shielded, hard wired CCTV devices, and wireless video devices that may be powered off. The inspection is conducted using a DLU-02 and the VORAN Concealed Video Camera Lens Detector. The VORON's LED matrix radiates a powerful infrared beam, which is then reflected by a video camera's optics, which can be easily detected by the operator. This inspection detects any optical device, whether it is powered or not, wireless or hard-wired. Two separate wavelengths of LED locate even those cameras with special coatings on the lens or lens filters.

Landline Telephone System Analysis:

This analysis includes both a physical and electronic examination of landline phone(s) and line(s), including instruments, incoming trunks, in-house cabling and peripheral equipment. Testing for intercept devices such as a phone or wiretap of landlines, including points of demarcation is included in this analysis. This inspection is conducted using a TALAN 3.0 Telephone and Line Analyzer. *(This analysis is performed when phone lines are included in the quoted services.)*

Physical and Electronic Examination of Computer(s) & Line(s):

We perform a physical and electronic examination of computer(s) and peripheral equipment for hardware technical surveillance threats. We also perform a survey for malware, spyware, screen capture, keystroke and remote monitoring software technical surveillance threats.

Wireless Network Analysis:

We perform an analysis of the Wi-Fi network using the NetScout G2 AirCheck Wireless Wi-Fi Analyzer and/or the ORIUS® Wi-Fi Hunter. The units provide a pass/fail indication of the wireless environment, identify common problems, analyze network utilization by channel, determine if it is 802.11 traffic or non-802.11 interference, and identify and locate wireless access points whether authorized or rogue, etc.

Cellphone Analysis:

Spyware/Malware: ComSec uses the SUSTEEN Data Pilot rugged field forensic acquisition device to quickly acquire time relevant evidence in the field, ad-hoc and list search, fast real-time reporting and to detect spyware/malware.

Cell Phone Forensics: ComSec's cell phone forensics service is a professional level service. Specifically, we use Cellebrite cell phone forensics technology, which is preferred by law enforcement, military and intelligence services. As well, all cell phone forensics services are performed by a Cellebrite Certified Mobile Examiners (CCME). The forensic examination with "on-demand" is used to search for viruses, spyware, Trojans and other malicious payloads in files on cell phone(s). *(This analysis may be performed at an additional charge.)*

GPS Tracking Device Detection:

We use the Andre Advanced Near-Field Detection Receiver, the Wideband RF Detector Pro-SL8, the Handheld Spectrum Analyzer HSA-Q1 and/or the Yorkie Pro to identify eavesdropping devices and GPS tracking devices on vehicle(s). The units detect and assist in locating nearby RF, infrared, visible light, carrier current and other types of transmitters.

ComSec LLC's TSCM / Cyber TSCM Services are conducted with the most current and most technologically advanced equipment. Please visit our Eavesdropping Detection Equipment page to learn more about our equipment and eavesdropping detection capabilities.

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 area of concern requires extraordinary OPSEC and additional inspection methods to be utilized

What Is Included with ComSec's TSCM / Cyber TSCM Services?

- A technical threat assessment.
- A comprehensive service using the most current and technological advanced TSCM equipment.
- An on-site debrief of our findings immediately following the service.
- On site assistance to locate devices and address vulnerabilities.
- An electronic report that includes the methods used, the results of the service and recommendations to improve your security posture.

How To Choose A TSCM / Cyber TSCM Service Provider

The Chosen Company Should:

- Be a professional company who specializes in providing TSCM / Cyber TSCM services.
- Be reputable, well established and willing to provide professional references.
- Have leadership who has extensive experience in TSCM / Cyber TSCM, counterespionage, counter surveillance and counterintelligence.
- Use inspection equipment that is current technology and designed to detect various types of eavesdropping threats.
- Utilize service teams that include very experienced, highly skilled TSCM / Cyber TSCM experts or specialists.
- Provide extensive training for service staff and ensure their competency in the use of the TSCM / Cyber TSCM equipment.
- Ensure service staff is educated on current eavesdropping devices, emerging threats and effective detection methods.
- Not have conflicting interests (e.g. does not also sell spy gadgets, does not sell or use GPS trackers, and/or does not conduct surveillance or bugging operations.)

ComSec LLC's History

About ComSec LLC:

J.D. LeaSure (CCISM), ComSec's President/CEO, founded the company in 2007. The Virginia based company was created to address a need for an expert TSCM service provider in the local area. In 2008, ComSec expanded services to USA nationwide. Demand for global counterespionage services grew, and ComSec met this demand. ComSec has enjoyed steady growth since opening. Learn more about ComSec.

ComSec forms strategic alliances with key service providers to offer the best solutions for our customers. We partner with cyber security, software, technology and related providers. This approach allows ComSec to focus on its core business. It also gives our customers options for a total solution.

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

About Our Leadership:

The driving force behind ComSec LLC is J.D. LeaSure, our President/CEO. His extensive counterespionage, counter surveillance, counterterrorism and counterintelligence knowledge is invaluable to the company and to the clients we serve. His distinguished career in these fields spans more than three decades and includes both work in the USA and globally. Learn more about J.D. LeaSure and the ComSec Team.

J.D. is also the Director of The Espionage Research Institute International (ERII) and a full member of the Technical Surveillance Counter Measures Institute (TSCMi). He is also an active contributor to the world of counterintelligence and technical surveillance countermeasures. Please view our Industry Affiliations to learn more.

Call Us At (800) 615-0392 To Schedule Your Service!