



**TECHNICAL SURVEILLANCE  
COUNTERMEASURES**

---

---

## ***Tell me about Comsec Associates.***

### ***Experience***

Since 1977 we have provided communications security, computer security, technical security, and electronic engineering consulting services to a broad and expanding range of clients. Our clients include major corporations, public utilities, leading law firms, federal government agencies, foreign diplomatic missions, law enforcement agencies, network news organizations, and financial services companies.

### ***Personnel***

We are staffed by personnel who have extensive training and experience in countermeasures, technical surveillance, communications, electrical and electronic engineering, and physical security.

### ***Standards***

Our greatest asset is the confidence of our clients. We always maintain the highest standards of professionalism, and assure our clients of the utmost discretion and confidentiality. We accept assignments only from legitimate, identifiable persons or entities. We do not accept assignments on criminal cases, nor do we accept assignments where involvement by the United States government or any law enforcement agency would be anticipated.

## ***Why should I be concerned about electronic eavesdropping?***

The current business climate is increasingly competitive. Many businesses are vying for the same customers, or to be the first in their field to bring a new or enhanced product to market. Many companies are having their very survival threatened by lawsuits. Companies are not even safe from their own employees, we commonly find eavesdropping being conducted by an ambitious employee seeking a more rapid path to promotion, or a disgruntled employee gathering company secrets in preparation of starting their own competing business.

Although industrial spying is unlawful, the rewards for procuring intelligence regarding the strategic plans, resources, products, pricing, customers, personnel, or legal affairs of a competitor often prove substantially more persuasive than concern over the risks involved in acquiring such information.

The security posture of businesses has been further complicated since the rise of capitalism in the republics of the former Soviet Union and in Eastern Europe. Agents of their once-feared foreign intelligence services are no longer seeking intelligence to further national political aims, they are now emphasizing the gathering of business intelligence to assist their struggling economies. This adds a new dimension to the long-time business intelligence gathering activities of myriad domestic and foreign corporations, and the governments of Israel, Japan, France, Argentina, Canada, Great Britain, Sweden, Switzerland, India, China, Taiwan, North Korea, South Korea, and Russia.

A 1992 study conducted by the American Society for Industrial Security (ASIS) found theft of proprietary information had risen 260% since 1985. In 1993 the FBI reported its industrial espionage caseload had jumped from ten to five hundred open cases. Any company in a business with foreign competition is a target for corporate espionage. R. James Woolsey, while Director of Central Intelligence, reported economics had become the hottest current topic in intelligence. The attitude of many nations, including his own, was explicitly stated by Pierre Marcon, former head of the French Direction Generale de la Securite Exterieur (DGSE), who said in an interview "In economics we are competitors, not allies."

Electronic spying is not confined to government agents. The equipment required for wiretapping and electronic eavesdropping is available to anyone through advertisements in the back pages of electronics magazines; and very sophisticated bugs can be constructed by anyone with a rudimentary knowledge of electronics, with components obtained from any Radio Shack store.

Favorite targets of industrial spies are technology, trade secrets, business plans, customer lists, and perhaps most damaging, pricing data. Any medium over which this data is transmitted, or location in which it is discussed, is vulnerable. We have found the preferred targets of industrial spies are often fax machines. These are especially attractive for intelligence gathering because information which was discussed over an extended period, possibly in multiple locations, is conveniently condensed and readily available in hardcopy form.



With the potential for, and severe consequences of, information loss, more and more prudent business and professional leaders are taking the precautions necessary to safeguard their sensitive and proprietary information.

---

---

## ***Why should I hire Comsec Associates?***

We have all seen the rapid advance of the state-of-the-art in high-tech consumer products, you purchase a new product and, seemingly by the time you get it home, it has been rendered obsolete by a newer, more advanced model. This is indicative of the advance of technology in all sectors, including the technical surveillance field. To keep up with the threat, you have to constantly research the state-of-the-art in commercially produced surveillance gear; and just as important, engage in a program of research and development to determine the adaptability of new technologies to the surveillance field.

Our engineers conduct an ongoing program of evaluation of new and emerging technologies. They analyze electronics trade publications, attend trade shows and seminars, and review manufacturers catalogs to determine what components or technologies might be applied to eavesdropping, and conduct further research with technologies of interest in our laboratories. This R&D program keeps us well positioned to counter eavesdropping threats from professionals armed with leading-edge surveillance equipment.

We have all the equipment necessary to conduct a thorough sweep, and always bring a full complement of equipment with which to perform all the analyses required for the completion of the countermeasures assignment. Our personnel have the training, knowledge, and experience to properly use this equipment to detect conditions which may indicate the presence of technical surveillance, and the understanding to thoughtfully analyze those conditions to determine whether there is actual cause for concern.

## ***How do you conduct a countermeasures survey?***

Our technical surveillance countermeasures (TSCM) surveys are conducted using meticulous procedures developed by our engineers. These procedures are constantly undergoing revision to accommodate innovations in surreptitious eavesdropping technology and methods. Our typical sweep includes, *but is not limited to*, the following.

### ***Radio spectrum and infra-red analysis.***

These analyses are conducted in two ways: during regular business hours, for the detection of remotely-controlled transmitters; and outside of regular business hours, close-in to the area of concern. To conduct the radio spectrum analysis we use a laboratory-grade *Spectrum Analyzer*, specially modified for TSCM, to detect transmitters operating well into the millimeter wave frequency range; and several high-quality *Receivers* to detect, demodulate, and identify all signals, including weak transmissions from other parts of the building. These receivers are capable of demodulating signals using amplitude modulation, frequency modulation, phase modulation, upper or lower side band modulation, frequency division multiplexing, subcarrier, or video; from VLF, well into the microwave frequency range. We also employ a sensitive infra-red optical instrument to detect and identify transmitters using infra-red LED's, or laser eavesdropping.

### ***Wiring analysis.***

We conduct a thorough analysis of telephone, electrical, and unidentified wiring for anomalous conditions with regard to capacitance, resistance, reactance, resistive imbalance, voltage, current flow, audio signals, digital signals, carrier current transmissions, and multiplexed emissions. Several pieces of proprietary equipment are used during this analysis, including a sophisticated *FFT Analyzer*.

### ***Telecommunications system analysis.***

We perform a meticulous physical inspection and analysis of your telecommunications systems, including the building entrance terminal, protectors, distribution frames, telephone switches, network demarcation blocks, aerial closures, distribution pedestals, underground service boxes, key systems, PBX, subscriber stations, riser closures, facsimiles, hubs, concentrators, routers, bridges, and every appearance of the protected circuits, both wire and fiber optic. We use several proprietary instruments for this analysis, as well as a *Time Domain Reflectometer* which provides both electronic and hard copy display of anomalous conditions in hidden wiring.

### ***Physical inspection.***

We conduct a thorough, methodical, physical search and inspection of the protected premises. This exhaustive search includes, but is not limited to, all crawl spaces, drop ceilings, floor coverings, furniture, fixtures, appliances, office equipment, books, and art objects. We also evaluate ducting, common spaces, and adjoining areas for acoustic transmission. During this search we employ a *Non-Linear Junction Detector* which will detect electronic devices, whether or not they are operating; a *Portable X-Ray* to thoroughly examine objects which may be damaged by physical inspection; a *Highly-Sensitive Thermographic Imaging System* to detect the faint heat emissions produced by operating electronic circuits, a *Magnetometer* to detect metallic shielding and components concealed in non-metallic objects; and *high-intensity ultra-violet illumination* to detect variations in painted surfaces, fresh putty, hidden wiring, or other modifications not usually visible under normal light. We also employ a *proprietary laser system* to detect concealed video cameras. Custom tamper-evident seals are placed on inspected items to assure you of their continued integrity.

### ***Report and security survey.***

Upon completion we provide a comprehensive report of our findings, with observations and recommendations to improve the security of sensitive information.

# **COMSEC ASSOCIATES**

**(818) 502-0000**

**(888) 202-2080**

**When you are serious about  
communications security.**

State License: PI-15830

**COMSEC ASSOCIATES, INC.**  
**P.O. Drawer 708**  
**La Canada Flintridge, CA 91012 U.S.A.**  
**(818) 502-0000**  
**(888) 202-2080**  
**[privacy@comsec.us](mailto:privacy@comsec.us)**  
**[www.comsec.us](http://www.comsec.us)**