Global Strategies, Inc.
Technical Surveillance Counter-Measures

The manufacture, sale, installation, and monitoring of illegal surveillance devices is a multi-billion dollar underground industry within the United States.

The U.S. State Department estimates that at least 800 million dollars of illegal bugging and eavesdropping equipment is imported and installed into corporations in the United States each year. The majority of this equipment is illegally imported into the United States from France, Germany, Russia, Lebanon, Italy, Canada, Israel, England, Japan, Taiwan, South Africa, and a host of other countries. Additionally, anyone with a soldering iron and a basic understanding of electronics can build and install an eavesdropping device. The raw materials to build such a device may be easily obtained at Radio Shack, or salvaged from consumer electronic devices such as cordless telephones, intercom systems, and televisions. Too tough? Check out the multitude of Junior Spy Kits ubiquitously sold at toy stores throughout the United States.

In the United States, over six millions dollars' worth of surveillance devices are sold to the public each day. Most of these products are sold from storefront operations, spy shops, attorneys, and via private investigators located in major metro areas such as New York, Miami, Los Angles, San Francisco, Dallas, Chicago, and Minneapolis. This does not include the tens of billions spent each year for legitimate eavesdropping products purchased by law enforcement, military, and intelligence agencies worldwide. This equipment is commonly sold over the counter, via mail order, and through the Internet. Most of these bugging devices cost only a few dollars, but highly sophisticated, quality products may be purchased for less than one thousand dollars.

The FBI and other federal law enforcement agencies have repeatedly indicated that they lack the resources and training to enforce or properly investigate the technical security threat within the United States. Law enforcement agencies, in general, lack either the training or equipment to perform bug sweeps.

The Objectives of any TSCM Program or Service

Detection - Measures taken to detect technical surveillance devices, technical security hazards, and physical security weaknesses that would permit the technical or physical penetration of a facility.

A technical surveillance device is an item designed to intercept conversations or electronic transmissions and is commonly known as a "bug."

A technical security hazard may allow the unintentional transmission of information, and is any condition which could permit the technical surveillance of an area. This condition may occur

with equipment due to its normal design, installation, operation, maintenance, component deterioration, or damaged condition. For example, some telephones have the ability to pass audio even when hung up.

Nullification - The process of neutralizing or negating technical devices employed by making the placement of such devices more difficult. This includes ensuring that a room is protected with adequate physical construction and security measures thus making the placement or use of illegal listening devices ineffective.

Isolation - A method to deter, or make extremely difficult, the introduction of an eavesdropping device by establishing special areas, security areas, or a Sensitive Compartmented Information Facility (SCIF's) for the conduct of classified or sensitive activities.

Services

TSCM Inspection - An evaluation (which does not involve test equipment) of a sensitive facility to determine what physical security measures are required to protect against technical penetration or unaided audio leakage.

In-Place Monitoring (IPM)- This is the simplest and lowest level type of legitimate TSCM sweep, it consists of monitoring a given thing or place while an event or meeting is in progress. While it is just a cursory check it's does allow a certain amount of security and privacy when time is limited. In- Place Monitoring assumes that the facilities are secure and that the only threat is from meeting attendees (i.e.: tape recorders, wireless microphones, etc...)

Protective Detail TSCM Survey/Sweep - Performed strictly for specific threat situations. This is the type of inspection the U.S. Secret Service performs for the President when he is going to be visiting a place. In addition to a full inspection, it also involves inspecting and X-raying walls, lamps, furniture, cushions, and so forth. The goal is to locate not only bugging devices, but anything that could cause the protectee any harm or embarrassment.

The amount of formal training needed to do this type of a sweep is very high, often involving years of training, and an extremely high level of expertise is required. Personnel providing this type of service will also be trained in some kind of executive and dignitary protection.

TSCM Preconstruction Assistance - A service conducted by TSCM personnel during the planning stages of new construction.

TSCM Screening - This inspection involves the examination of equipment and furnishings prior to their introduction into a facility which has previously received a TSCM survey