The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE

Summary

1. Pre-inspection discussion and orientation.
2. Visual examination.
3. Technical inspections.
4. Information security survey.
5. On-site debriefing.
6. Written report.

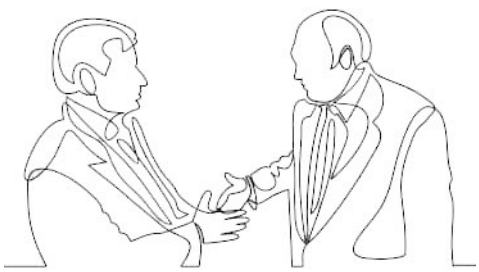
Our most commonly-used procedures and instrumentation are listed below. The specific procedures and instrumentation we use for your inspection are custom crafted based upon your particular: concerns, location, security goals and communications systems.

The search process is constructed so that our tests overlap each other in effectiveness, thus automatically creating a double-check analysis strategy.

1. Pre-Inspection

We discuss, in confidence: suspicious incidents you may have observed, your security concerns, and your goals for a successful resolution. During follow-up inspections we review interim information and discuss the implementation of security recommendations made during previous inspections.

Upon arrival an initial walk-through orientation of the areas being inspected provides us with information about: access control, building construction, room contents, distances between areas, locations of IT/telecom rooms, etc.



All of this diagnostic information is used to plan our inspection strategy, and select the most effective test procedures to successfully resolve your concerns.

The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE

2. Visual Examination

A thorough physical examination is conducted to discover electronic surveillance devices currently in place, *and* any evidence of prior eavesdropping attempts. This phase of the inspection includes a detailed examination of: furniture; fixtures; wiring; ductwork; computers, and small items within the area.

Our TSCM physical inspections are enhanced using the latest technology: hi-res CCTV, laboratory grade thermal imaging, advanced Non Linear Junction Detection (NLJD), additional tools, and manual inspection techniques. This is how we discover eavesdropping devices which do not use radio-frequency transmission.

Examples include:

- miniature voice recorders,
- sound extraction via direct wiring,
- carrier current over power lines,
- transmissions using infrared light,
- ultrasonic and laser microphones,
- covert video spycams with internal SD cards,
- and keystroke loggers.

These eavesdropping devices may be secreted in hollow walls, behind false ceilings, in or on furniture, fixtures and other common items which have a legitimate place in the room, such as: computers, power strips, radios and clocks.

3. Technical Inspections

DETECTION OF NON-RADIATING DEVICES

Surveillance devices do not have to be transmitting, or even turned on, for us to discover them. The Non-Linear Junction Detection instrumentation we use can detect bugs operating in their standby mode, on timers, or even with dead batteries.

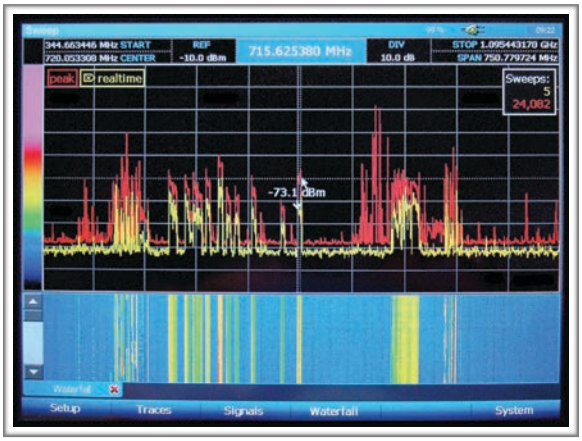
This detection technology is similar to the shoplifting detectors used at retail store exits. Just the fact that the bug is using electronic components is enough to sound the alarm.

Non-Linear Junction Detector

The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE

RADIO RECONNAISSANCE SPECTRUM ANALYSIS® (RRSA)



Detection and demodulation of wireless surveillance (audio, video & data) is accomplished with the aid of government-level computerized spectrum analyzers.

RRSA® detection is very sensitive. Even though only certain areas of a building are designated for inspection, surrounding areas also benefit from this particular test.

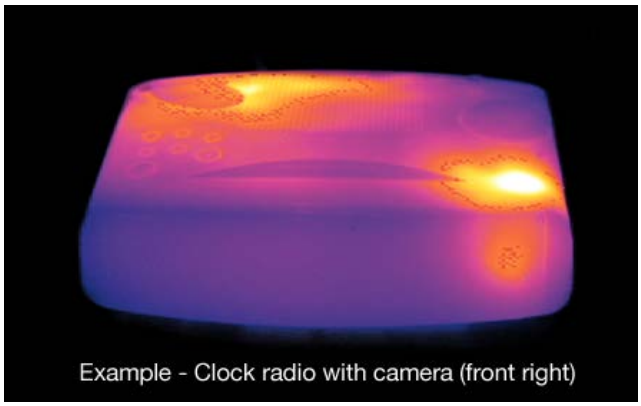
OPTICAL EMISSIONS SPECTRUM ANALYSIS® (OESA)

Some electronic eavesdropping devices transmit intelligence by converting sound into infrared or laser light. This invisible light can be picked up optically from a distance and converted back into sound. (The average television remote control operates using the same principle.) Our instruments can detect this.

CONCEALED SPACE EXAMINATION

Spaces which cannot be directly viewed are optically examined using a flexible videoscope, similar to the one pictured on the right.

THERMAL EMISSIONS SPECTRUM ANALYSIS® (TESA)



Example - Clock radio with camera (front right)

Minute amounts of heat are generated as electricity moves through a surveillance device's circuitry. Our laboratory grade TESA® instrumentation allows us to detect active items. This technique can also see bugs hidden in antique furniture and other delicate items – without damaging them.

In addition to the above procedures, we may employ some other specialized tests, based on your unique needs.

The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE

HARD-WIRED COMMUNICATIONS EXAMINATION

- Visual inspection of the individual system components and connecting pathways.
- Frequency Domain Reflectometery (FDR) Analysis of the wiring paths.
- Carrier Current Analysis of the wiring paths.
- Audio Leakage Analysis.
- Electrical Characteristics Analysis.

Advanced Communications Analyzer

WIRELESS COMMUNICATIONS EXAMINATION

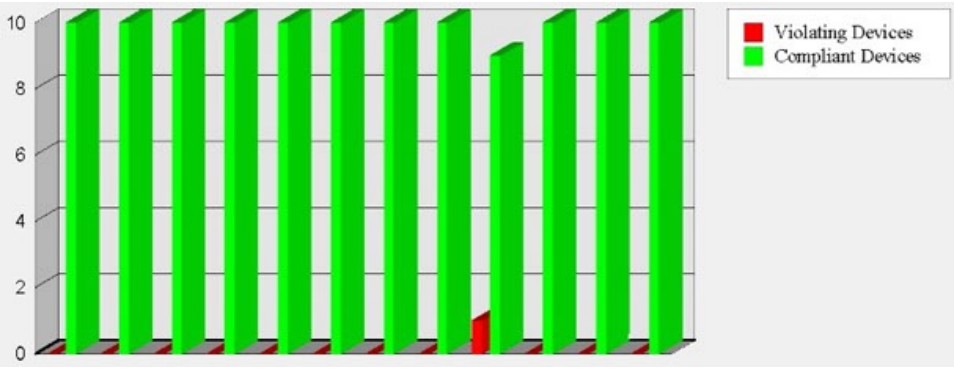
- Cordless telephones.
- Wireless headsets, keyboard and mice.
- Wireless presenter's microphones.
- Other wireless communications (Bluetooth, FM Analog, etc.)

WIRELESS LAN (WI-FI) SECURITY AND COMPLIANCE AUDIT

A Wi-Fi security and compliance audit is an essential element of our TSCM inspection process. It lets us detect WiFi-reliant audio and video covert surveillance, and rogue network intrusion devices, in addition to compliance issues. This inexpensively helps guard against eavesdropping, data siphoning and government penalties due to compliance lapses.

Although a Wi-Fi inspection is part of our TSCM service, it may be ordered separately when Wi-Fi security and compliance are the sole concerns.

Just one loophole...



Hackers are in. Data is out.
&
"*You are out of compliance.*"

The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE

Some privacy laws and directives which may impact your Wi-Fi usage include

- Sarbanes-Oxley Act – U.S. Public Companies
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach-Bliley Financial Services Modernization Act
- PCI-DSS – Payment Card Industry Data Security Standard
- FISMA – Federal Information Security Management Act
- DoD 8100.2 – Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid
- ISO 27001 – Information Security Management
- Basel II Accord – Banking
- EU - CRD (Cad 3) – EU - Capital Requirements Directive - Banking

TAMPER DETECTION

Government grade security seals are used to seal phones and other objects after inspection. Items previously inspected and sealed are re-examined by us to verify seal integrity. The seal numbers are recorded in our written report.

Our security seals are custom-made especially for Murray Associates. The unusual fluorescent security ink in the circle design is not easily duplicated.

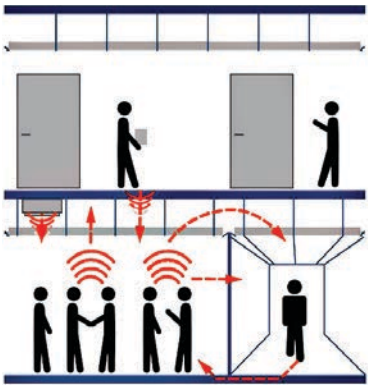
Between inspections you should visually examine these seals yourself. A damaged or missing seal may indicate tampering. A missing seal may also indicate the object being sealed was replaced with a pre-bugged identical-looking item. Either condition is a suspicious incident which should be investigated further.

ACOUSTICAL DUCTING EVALUATION

This phase of the inspection evaluates the possibility of sound migration — a sometimes surprising cause of information loss.

Ductwork, open ceiling plenums, common walls/ceilings/floors can conduct sound in unexpected ways.

Our recommendations will help you prevent this type of unnecessary information loss.



The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE

4. Information Security Survey

As part of our inspection process we observe general security efforts already in place, to assess appropriateness and current effectiveness. Items observed include:

- CCTV, locks, alarms.
- Employee compliance with good information security practices.
- Access control.
- Security officer efficiency.
- Potential for abusing in-place technologies.
- Security policies (in place, or needed).
- General security and safety observations.

(Video examples… https://counterespionage.com/tscm-video/)

Cost-effective recommendations for improvements, repairs, upgrades, and additions are made as necessary. Since we don't sell, or profit in any way, from products and services we recommend, you are assured our recommendations are in your best interest.

5. Debriefing

An immediate debriefing to discuss the results of our inspection, urgent security items, and future strategy are discussed at this time.

6. Written Report

Our written counterespionage report documents your security inspection, and due diligence. It may also contain recommendations requiring your immediate attention.

Maintain a cautious attitude and safeguard your report. It discusses security strategies which are not for general dissemination. It also documents your proactive stance and due diligence on information security – a legal prerequisite for protection in court.

Thank you for considering our services. If you have any questions, or would like to create an effective security strategy, just let me know.

Kevin

Kevin D. Murray, CPP, CISM, CFE
908-832-7900
murray@counterespionage.com