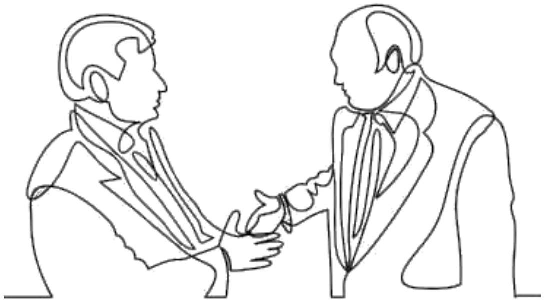
Murray Associates | Security Report

The TSCM Inspection Process

by Kevin D. Murray, CPP, CISM, CFE, CDPSE



Summary

1. Discussion, evaluation and planning.
2. Detailed visual exam of sensitive areas.
3. Technical inspection of the areas.[1]
4. Information security survey.[2]
5. A post-inspection debriefing.
6. A final written report documenting findings, recommendations and due diligence.

The most commonly used procedures and instrumentation are listed here. 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 Technical Surveillance Countermeasures (TSCM)[3] portion of our inspection process is constructed so that procedures 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.
- 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.

2. Visual Examinations

A thorough physical examination is conducted to discover electronic surveillance devices currently in place, and any evidence of prior eavesdropping attempts.

[1] https://counterespionage.com/tscm-technology/

[2] https://counterespionage.com/advanced-tscm-explained/

[3] https://en.wikipedia.org/wiki/Countersurveillance

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, thermal imaging,[4] advanced Non Linear Junction Detection[5] (NLJD), additional tools, and manual inspection techniques. This is also how we discover eavesdropping devices which *do not* broadcast radio-frequency transmissions.

Examples include:

- miniature voice recorders,
- transmitters which may be dormant, or have dead batteries,
- sound extraction via direct wiring,
- carrier current over power lines,
- transmissions using infrared light,
- ultrasonic and laser microphones,
- covert spycams with internal SD cards,
- keystroke loggers.
- and a malicious USB cable inspection, and certification of authentic cables.[6]

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 Examinations

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.

Radio Reconnaissance Spectrum Analysis® (RRSA)

Detection and demodulation of wireless surveillance (audio, video & data) is

[4] https://counterespionage.com/tscm-technology/thermal-emissions-spectrum-analysis/

[5] https://counterespionage.com/tscm-technology/non-linear-junction-detection-nljd/

[6] https://counterespionage.com/malicious-usb-cables/

accomplished with the aid of government-level, computerized spectrum analyzers.

RRSA® detection is very sensitive. Even though only certain areas of a building may be 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 instrumentation 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®

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.

Internet of Things Exam

The Internet of Things (IoT) has introduced many not-so-obvious attack points into businesses. From printers to VoIP phones to AV presentation equipment, all are taken into consideration during the TSCM inspection process.

Hard-wired Communications Examination

- Visual inspection of system components and connecting pathways.
- Frequency Domain Reflectometery (FDR) Analysis of the wiring paths.
- Carrier Current[7] analysis of wiring.
- Audio leakage analysis.
- Electrical characteristics analysis.
- Advanced communications analyzer.

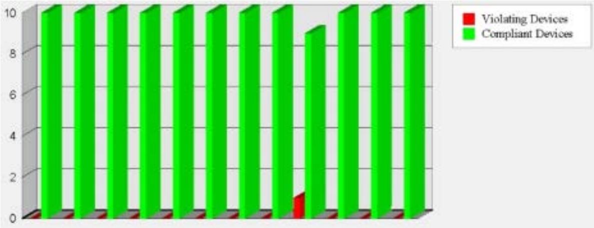
Wireless Communications Examinations

- Wi-Fi security and compliance analysis.
- Cordless telephone vulnerabilities.
- Cordless headsets, keyboard and mice.
- Wireless presenter's microphones.
- Other wireless communications (Bluetooth, FM, analog, etc.)

[7] https://en.wikipedia.org/wiki/Carrier_current

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. Additionally, our test can detect compliance issues.



Just one loophole…
Hackers are in. Data is out.
&
"You are out of compliance."

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.

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

Tamper Detection

We use government grade security seals to seal phones and other objects after our 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 may 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, possibly 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—sometimes a surprising cause of information loss.

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

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

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)[8]

We provide cost-effective recommendations for improvements, repairs, upgrades, and additions, 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. On-Site Debriefing

An immediate debriefing can be held to discuss the results of your inspection. Urgent security issues, and future protection strategies are discussed at this time.

6. The Written Report

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

We ask our clients to maintain a cautious attitude, and safeguard the 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, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[9] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[8] https://counterespionage.com/tscm-video/

[9] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/