

The TSCM Inspection Process

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



Summary

Pre-inspection

1. Discussion and evaluation.
2. Strategy and estimate creation.¹
3. Scheduling the inspection.

On-site

4. A detailed visual examination.
5. A technical evaluation.
6. An information security evaluation.
7. A post-inspection debriefing.

Post-inspection

8. A comprehensive written report is typically submitted within a week.

Introduction

We discuss, in confidence, your security concerns, goals, and any suspicious incidents you may have observed. Like a visit to the doctor, these form the inspection strategy. Our choice of tests and instrumentation required for a successful outcome is based on this.

On Site

An initial walk-through orientation of the areas being inspected provides us with more insights about: access control, building construction, room contents, distances between areas, locations of communications equipment rooms, etc. This additional information is used to refine our inspection strategy.

The most commonly used TSCM procedures and types of instrumentation used are described in the following sections.

Visual Examination

Visual examinations discover electronic surveillance devices currently in place and note evidence of prior surveillance device placements.

This phase of the inspection includes examinations of: furniture; fixtures; wiring; ductwork; and small items within the area.

Instrumentation such as: Wi-Fi/Bluetooth and radio-frequency spectrum analyzers, thermal imaging,² Non Linear Junction Detection³ (NLJD), aid the process.

The last two techniques assist in discovering surveillance devices not broadcasting at the moment or at all.

Examples of this include:

- miniature voice recorders,

¹ <https://counterespionage.com/estimate/>

² <https://counterespionage.com/tscm-technology/thermal-emissions-spectrum-analysis/>

³ <https://counterespionage.com/tscm-technology/non-linear-junction-detection-nljd/>

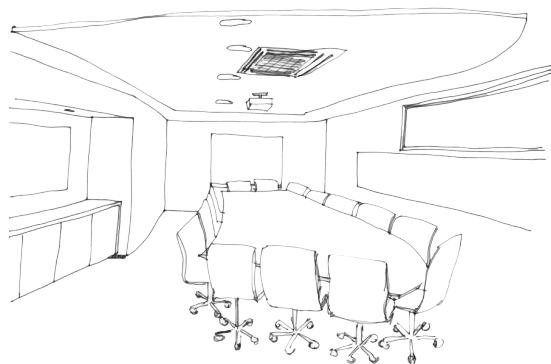
The TSCM Inspection Process

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



- 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 cables.

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.



Technical Instrumentation

The Technical Surveillance Countermeasures (TSCM) portion of your inspection is constructed so that procedures overlap each other in effectiveness automatically creating a double-check analysis strategy.

Non Linear Junction Detection

Surveillance devices do not have to be transmitting or even turned on for us to discover them.

Non-Linear Junction Detection 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 contains electronic components is enough to sound the alarm.

Radio Reconnaissance Spectrum Analysis

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

These receivers are very sensitive. Even though only certain areas of a building may be designated for inspection, surrounding areas also benefit from this particular test at no additional cost.

Optical Emissions Spectrum Analysis

Some surveillance devices transmit their intelligence by converting the information into infrared or laser light. This invisible light can be picked up optically from a distance and converted back into sound.

Television remote controllers operate using this communications via light principle. Our instrumentation can detect this.

Video Inspection

Spaces which cannot be directly viewed, such as false ceilings and small spaces, are optically examined using a pole mounted camera or flexible videoscope.

The TSCM Inspection Process

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



Thermal Emissions Spectrum Analysis

Minute amounts of heat are generated as electricity moves through a surveillance device's circuitry. Our instrumentation allows us to detect these 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 can employ additional specialized tests, based on your unique needs.

Internet of Things

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.

Wired Communications

Multiple tests are available for testing wiring. These include:

- Visual inspection of system components and connecting pathways for attachments.
- Frequency Domain Reflectometry (FDR) to detect unexposed attachments.
- Carrier Current⁴ analysis of wiring.
- Audio leakage analysis.
- Electrical characteristics analysis.
- Advanced communications analysis.

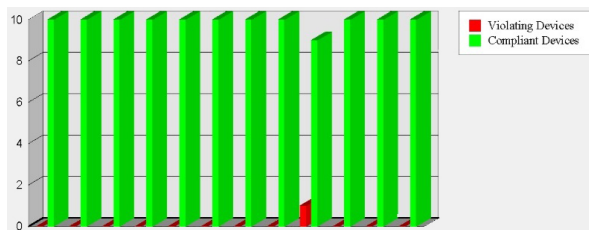
Wireless Communications

Wireless device vulnerabilities are evaluated. These include:

- Cordless products which transmit radio signals, such as: telephones, headsets, keyboards, and input devices.
- Wireless presenter's microphones.

Wi-Fi Security and Compliance Audit

This is an essential element of the TSCM inspection process. It detects WiFi-based audio and video covert surveillance, and rogue network intrusion/exfiltration devices. Compliance issues are also identified.



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

Tamper Detection

Serial-numbered security seals are often used to seal phones and other objects after inspection. On follow-up inspections, items previously inspected and sealed are re-examined to verify seal integrity.

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.

⁴ https://en.wikipedia.org/wiki/Carrier_current

The TSCM Inspection Process

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



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.

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/safety observations.⁵

Cost-effective recommendations for security improvements, repairs, upgrades, and additions will appear in the written report.

Note: 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.

On-Site Debriefing

An immediate post-incident debriefing may be held to discuss our findings. Urgent security issues and future protection strategies are discussed at this time.

Written Report

A written report documents your inspection and due diligence. 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.

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 D. Murray CPP, CISM, CFE, CDPSE is a technical information security consultant and TSCM specialist with over four decades of experience.

Murray Associates⁶ is an independent security consulting firm, providing eavesdropping detection and counterespionage services to businesses, governments, 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.

⁵ <https://counterespionage.com/tscm-video/>

⁶ <https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/>