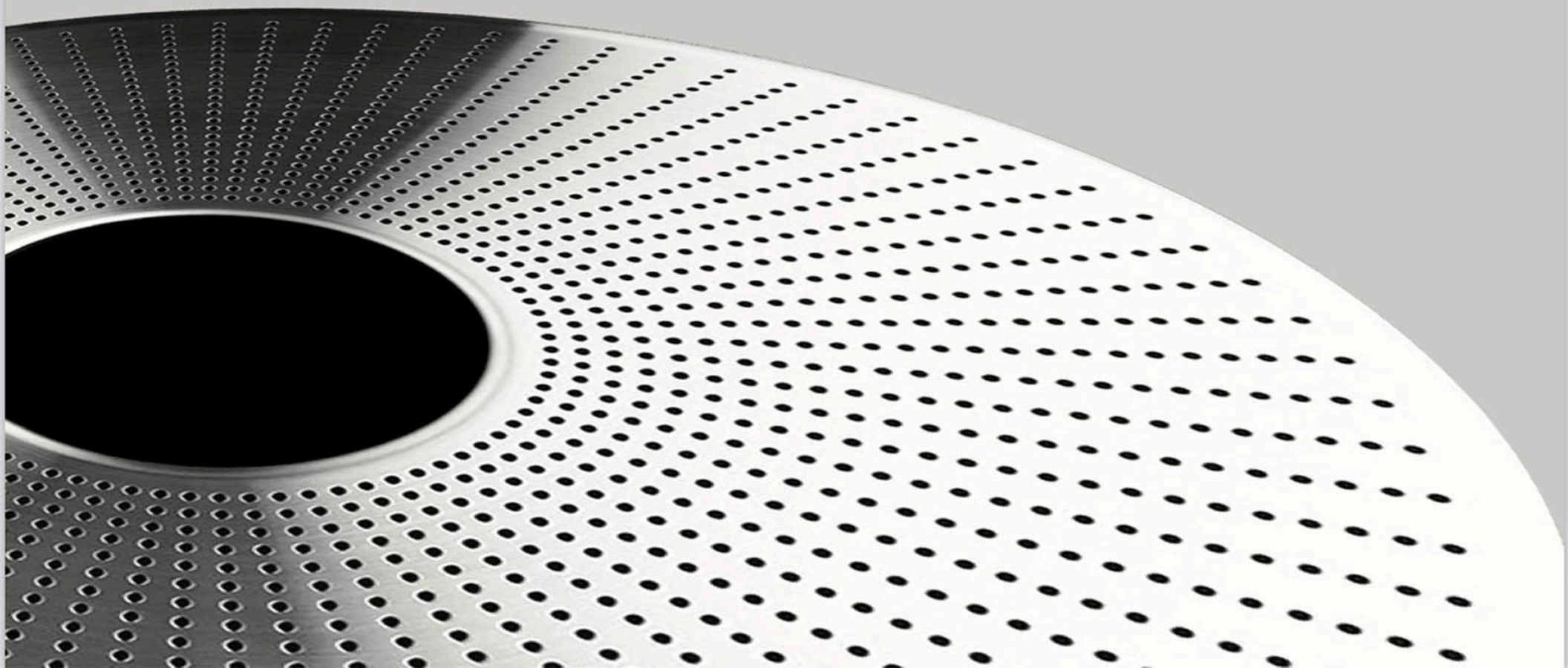




Murray Associates

**The
Security Director's
Guide to Discussing
TSCM**
with Management



Bugs Live Here...



● Boardrooms

● Trading floors



● Executive suites

● Conference rooms

● Corporate apartments



● Vehicles, aircraft & yachts

● Quarterly Board Meetings



● Executive homes & offices

● Wi-Fi security & compliance



● Expectation of Privacy areas

● Hotel rooms & conference centers

Contents

Foreward	4
Introduction to TSCM	4
Management Wants to Know	5
“ What is TSCM? ”	5
“ What’s the risk? ”	5
“ What do TSCM inspections protect? ”	6
“ Do we legally need this type of security? ”	6
“ What are the benefits? ”	7
“ Who will conduct the Inspections? ”	7
Outsourced TSCM Inspections	8
In-house TSCM Inspections	9
Hybrid TSCM Inspections	11
The Inspection Explained	13
Elements Common to Most Inspections	14
Moving Forward	16
Selecting Your Consultant	16
Plan a Strategy	16
“ Will I receive a written report? ”	18
“ How do we schedule inspections? ”	18

Foreward

Introduction to TSCM

Technical Surveillance Countermeasures (TSCM) began as a military term for electronic surveillance detection inspections. In the business world we take a more holistic approach. TSCM now means identifying all vulnerabilities related to information generation, transmission and storage—audio, video and data.

People turn to you for security guidance and advice. They expect you to know about eavesdropping detection, spy cameras, GPS tracking, and how to keep the competition from stealing information (counterespionage). They look to you for the truth about these unsettling business and personal issues.

You help them by providing accurate information and sound advice. Doing this automatically increases your reputation and credibility. This guide will help you accomplish all these things.

—Kevin D. Murray

Management Wants to Know

“What is TSCM?”

TSCM is an acronym for **Technical Surveillance Countermeasures**; an inspection to detect and protect against illegal electronic surveillance.

You may also want to mention:

- Inspections are a standard business practice.
- Often conducted quarterly, or biannually.
- Not disruptive, can be conducted after-hours.
- TSCM inspections provide a regular opportunity to spot other security vulnerabilities like office technology loopholes, security hardware failures, and non-compliance with policies.

“What’s the risk?”

- Strategy Spying
- Mysterious Leaks
- Business Espionage
- Internal Intrigue
- Malignant Activism
- Competitive Intelligence
- Media Snooping
- Adverse Publicity
- Blackmail
- Revenge
- Personal Privacy (audio eavesdropping, and spy cameras in expectation-of-privacy areas)

Electronic surveillance is silently at the core of many business problems.

“What do TSCM inspections protect?”

- Sensitive Communications
- Boardroom Discussions
- Mergers & Acquisitions
- Delicate Negotiations
- Lawsuit Strategies
- Executive Suites
- Personnel, Sales, Marketing, and Legal Departments
- Trade Secrets
- Personal Privacy
- Vulnerable Off-Site Meetings
- Wireless Local Area Networks (Wi-Fi / WLANS)
- Executive Residences & Home Offices
- Vehicles—including airplanes and yachts

“Do we legally need this type of security?”

An attorney should answer, but consider...

- Fiduciary Responsibility to stockholders.
- Duty of Care to protect trade secrets, intellectual property and strategic communications.
- Due Diligence requirements.
- Fulfilling the legal requirements for business secret status in court.
- Wi-Fi and information security compliance with:
 - HIPA - FISMA - DoD 8100.2 - ISO 27001
 - GLBA - PCI-DSS - Sarbanes-Oxley Act

“What are the benefits?”

- Increased profitability.
- Intellectual property protection.
- A *known* window-of-vulnerability when a bug is discovered.
- The ability to discover and plug information loopholes *before* they are abused.
- Advance warning of intelligence collection activities.
- An assessment of how current security measures and policies are being followed.
- Documented compliance with privacy laws.
- Fulfilling the requirements for obtaining "Business Secret" status in court will be easier.
- Enhanced personal privacy and security.
- Employees feel their privacy is protected.
- If employees see management cares about information security, they will care more too.
- Knowledge of office technology hacking vulnerabilities, and what to do about it.
- Reduction of consequential losses, *e.g.*, an information leak sparks a stockholder's lawsuit, or... activists releasing wiretap recordings to damage good-will and sales.

“Who will conduct the inspections?”

You have three choices...

1. Outsource to an independent TSCM specialist.
2. Develop an in-house capability.
3. Develop a hybrid program.

Outsourced TSCM Inspections

- No payroll or benefit expenses.
- Zero capital investment in expensive instrumentation.
- No expensive and time-consuming training... for your employees.
- Access to specialized expertise and advice.
- A broad range of field experience is applied to your concerns.
- A specialist's recommendations can fortify your own recommendations to management.
- Fresh eyes observe more.
- No vested interest in company or personal information they may see.
- No risk to your reputation.

Quality TSCM consultants also offer...

- Informative White Papers
- Expert Witness Capability
- Customized TSCM Training
- Valuable Second Opinions
- Information Security Surveys
- Counterespionage Consulting
- Complimentary Security Alerts
- Independent Recommendations
- Product Research and Evaluations
- Office Technology Vulnerability Assessments

To make your job easier and make you look good.

In-house TSCM Inspections

Having someone in-house who can conduct a TSCM inspection is very convenient in several instances, such as...

- Providing a quick response to last-minute inspection requests.
- The ability to handle minor requests such as checking a single hotel room or conference room.
- Frequent inspections of expectation of privacy areas; restrooms and vehicles, for example.

Most organizations, however, have phased out their in-house TSCM efforts. There are several good reasons for this...

1. Executives are sensitive about their privacy.

A secure environment that provides privacy is essential. Executives want to be protected against electronic surveillance. And, they want their offices to be professionally inspected, not violated.

An outside professional TSCM specialist...

- Won't repeat private correspondence seen.
- Won't play with the shelf toys.
- Won't comment on family photos.
- Will leave everything exactly as they found it.

With this in mind you, can understand why executives might worry about employee conducted inspections becoming snoop-fests.

2. These are not your father's surveillance devices.

Sophisticated eavesdropping and recording devices these days may be easily and cheaply purchased in a wide variety of excellent covert disguises. An in-house TSCM physical inspection by an amateur is doomed to miss all but the most obvious surveillance attempts.

Corporate headquarters executive floors are now showplaces of technology. In-house TSCM inspections of these areas are not just inadequate, they are borderline negligent.

3. Initial training is soon forgotten.

Let me share one of our experiences with you...
A few years ago, a client who had an in-house TSCM program called us in to provide training for their team.

The company had purchased equipment and initial training from a manufacturer 3-4 years prior. They were long overdue for a refresher course.

Upon sitting down with them we discovered their spectrum analyzer (same model as ours) was working at only 30% sensitivity. I was told, "It always worked this way." They weren't aware the receiver was deaf.

Even the most sincere in-house TSCM techs have these issues working against them...

- Retaining initial training takes practice.
- Keeping up takes continuing education.
- Developing a depth of experience requires a diversity of inspection situations.

4. Human nature.

Everyone is eager and excited when beginning a new in-house TSCM program. This soon fizzles out.

Physical searching involves bending, stooping, looking under tables, and climbing ladders. This is hard work; work for which not everyone is suited, or likes.

Consider the reality...

- If you give someone more work, longer hours, they will want a raise and compensatory time off. No money. No time off. No diligent searching. The inspection becomes a mental security band-aid.
- Inspecting the same, limited environment over and over again is mind-numbing.
- If you give someone the job of finding something they can't recognize even if they see it, they will think, "Nothing to see, so why look."

5. "An in-house TSCM effort is cost-effective."

Cost effectiveness won't matter when you suffer a loss due to ineffective in-house TSCM efforts. Every espionage loss is an expensive loss.

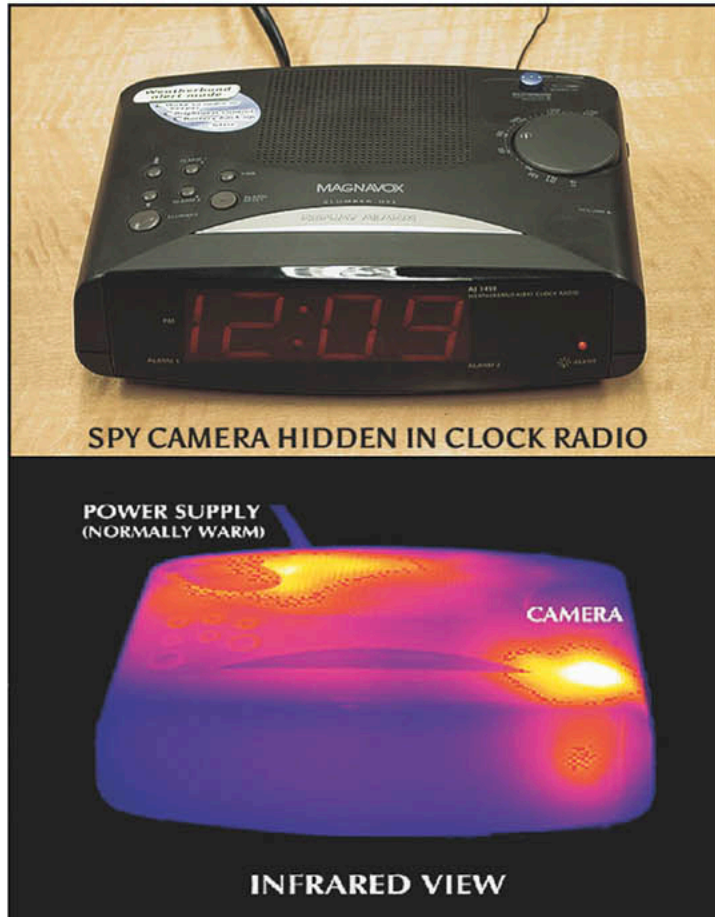
Hybrid TSCM Inspections

This type of program consists of an in-house employee working in conjunction with an independent TSCM specialist.

A hybrid program mitigates the problems associated with a 100% in-house effort, while retaining some of its key benefits.

The hybrid model works like this...

1. The TSCM specialist conducts the in-depth inspections on a scheduled basis.
2. Your employee receives enough training from the specialist to conduct summary inspections with minimum instrumentation.
3. The employee relies on the specialist to remotely advise them should a question or problem arise.



The Inspection Explained

Every TSCM inspection is individually crafted to suit the situation, but it generally goes like this...

Arrange a mutually convenient time to conduct your inspection. Most TSCM providers will schedule their services any time of the day, including weekends and most holidays—at no extra charge.

They should handle all the travel arrangements for you. You simply pick a time and date. One exception might be an off-site meeting. You may want to include them on your master billing if you have a group rate.

Upon arrival you may want to further discuss your concerns, goals and any late-breaking events. This is also a good time for an orientation tour.

In the movies, bugs and wiretaps are quickly located. Clever actors seem to know just where to reach under the table. The more technically oriented are equipped with the obligatory bug finding “ubergadget”, fresh from the lab.

Real-life inspections are conducted a differently. Information (visual, audio and data) is extracted from sensitive areas in a variety of ways.

There is no “one” test or gadget that will detect all bugs. The inspection protocol is aided by a variety of specialized instrumentation...

Elements Common to Most Inspections

- **Radio-Frequency Spectrum Analysis**

A search for surveillance devices which transmit information via radio waves.

- **Infrared Spectrum Analysis**

Detection of the heat emitted by spycams, bugs and other electronic circuits. Heat signatures may be seen even when these devices are hidden within ceiling tiles, walls, or furniture.

- **Communications Analysis**

A group of tests which identify surveillance methods used against: telephones, Wi-Fi printers, teleconferencing equipment, faxes, computer networks, and copy centers.

- **Mapped Physical Inspection**

Each area is combed with several objectives in mind: locate hidden surveillance devices; locate evidence of prior installations; note future surveillance vulnerabilities; and report other security issues discovered.

Example:

A clear thread seen in a drape or carpet may look normal. Knowledgeable TSCM investigators will suspect a fiber optic microphone and inspect further.

- **Non Linear Junction Detection**

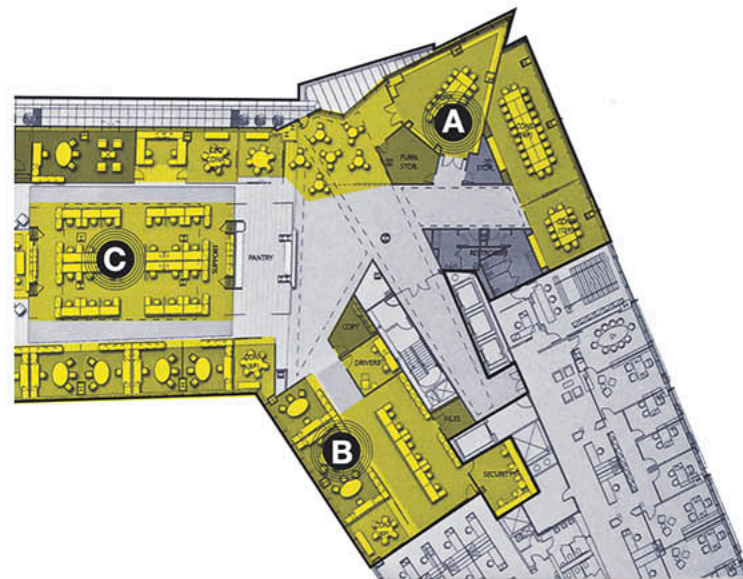
Areas are re-examined using a technique which reveals semiconductor electronic components (transistors, diodes, etc.), the building blocks of electronic surveillance devices. Devices hidden in

other objects can be located with this technology—even if they are not powered during the inspection!

- **Additional tests...**

Each of the basic inspection elements also contain sub-tests. Spectrum Analysis, for example, is not simply an inspection of radio frequencies. Light wave frequencies can also move sound.

Similar to other diagnostic crafts, e.g. the medical profession, inspections are crafted by selecting the appropriate tests for each situation.



Moving Forward

Selecting Your Consultant

Visit lots of websites. Avoid ones overusing scare tactics, bug and sweep gear photos, vague claims, and ones lacking curriculum vitae or resumes. Conduct interviews, then select the right person.

Read *How to Choose a Competent TSCM Consultant*¹ for a list of interview questions you should ask.

Plan a Strategy

- **Discuss your concerns, goals.**
Do this in/from a *safe* area, of course. Begin with non-disclosure agreement created by your legal counsel.
- **Create a priority list.**
Focus attention on the most sensitive areas first. This keeps costs low without sacrificing your goal—keeping information where it belongs. Provide a floor map. You will receive a more accurate cost estimate if you do.

Bonus: The radio-frequency and Wi-Fi elements of TSCM inspections cover wider areas by default—at no extra cost.

¹ <https://counterespionage.com/competent-tscm-consultant/>

- **Plan a schedule of follow-up inspections.**
Most organizations find quarterly or biannual inspections suit their needs. Some use a mixture of both—some areas inspected quarterly and others just biannually. Risk levels vary. Other layers of security, like access control and current activity, will influence the decision.

Schedule supplementary inspections for your off-site meetings, board meetings, periods of elevated risk and unexplained information losses as needed.

- **Ask for a detailed written proposal.**
It should list the scope of the inspection, line-item cost, inspection process, and how the findings will be reported.



“Will I receive a written report?”

Yes, make it clear you want a full written report in a timely manner. Do not pay for the inspection before you receive it.

The report should include:

- locations inspected,
- devices inspected,
- the inspection methodology,
- instrumentation used,
- information security issues discovered,
- findings and general observations,
- and recommendations for remediation.

Photographs and floor maps of the areas inspected should also be included, as appropriate.

Ideally, your inspection report should be written by an independent and credentialed security consultant.

Besides being proof of your due diligence, the writer *and* the report should be unassailable in court.

“How do we schedule inspections?”

- Contact your chosen professional from a “safe” phone. Tell them about your organization’s concerns and goals. Ask for their advice on what to inspect and how often.
- Request their Fee Schedule and a written estimate, including expenses.
- Decide upon a mutually convenient inspection date and time.
- Have keys to any locked rooms, contiguous areas, phone closets, etc.

- Have a step ladder available, if possible.
- If an incident has occurred, collect as much background information as you can. This will help your consultant solve your problem.

Until then...

- Do not discuss the inspection in, or call from, suspect areas.
- Conduct your affairs normally.
- Do not reveal any suspicions, except on a real need-to-know basis.
- Limit confidential conversations.
- Keep detailed notes about anything you feel is suspicious.
- Think ahead. What if a device is found by an employee accidentally? Have a protocol in place so the situation is properly handled.²

Congratulations. You can now discuss technical surveillance countermeasures with management, confidently and intelligently.

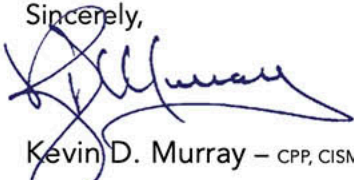
² <https://counterespionage.com/found-a-bug/>

Murray Associates, founded in 1978, is an independent consulting firm specializing in electronic surveillance detection (TSCM) and counterespionage consulting.

We work with security directors—as *technical security consultants*—so you can provide these specialized services to your organization.

Thank you for considering our services.
All of us here look forward to working with you.

Sincerely,



Kevin D. Murray – CPP, CISM, CFE, MPSC



R.S. Please contact us directly if this guide does not answer all your questions.

OPERATING POLICY

MURRAY ASSOCIATES is a security consulting firm which limits its services to the: prevention of unlawful electronic surveillance; the protection of privacy; and the prevention of information theft.

We will endeavor to:

- Assure absolute confidentiality.
- Provide the most knowledgeable and effective services at a fair cost.
- Remain unbiased in our efforts and recommendations.

We will not accept assignments:

- Without a clearly stated purpose.
- To obtain privileged information.
- Which are against the best interests of the U.S. government or its citizens.

— Kevin D. Murray, 1978