Murray Associates

The Security Director's Guide to Discussing TSCM with Management

Contents

Greetings

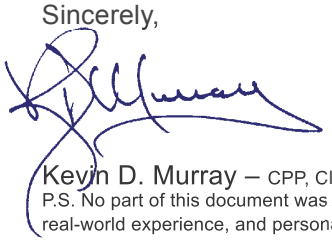
Murray Associates, founded in 1978, is an independent consulting firm specializing in Technical Information Security Inspections. This is a more advanced and complete form of the dated TSCM bug sweep.

We work with people having security responsibilities, most likely you, so you can provide this specialized service to your organization.

People turn to you for security and privacy advice. They expect you to know about eavesdropping detection. They look to you for the truth. Providing them with accurate information and sound advice increases your reputation and credibility. This guide will help you do that.

Always feel free to contact me if you still have questions.

Sincerely,



Kevin D. Murray – CPP, CISM, CFE, CDPSE
P.S. No part of this document was AI generated. It contains personal knowledge, real-world experience, and personally created artwork only.

LinkedIn https://www.linkedin.com/in/kevindmurray1/

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

Introduction to TSCM

Technical Surveillance Countermeasures (TSCM) is an inspection to discover unauthorized electronic surveillance. In the business world the concept has a broader benefit. It includes pro-actively identifying additional types of espionage and information security vulnerabilities. Better than espionage insurance, it can prevent the loss in the first place.

"What is TSCM?"

TSCM, originally a military acronym for **Technical Surveillance Countermeasures**; basically; an inspection to detect unauthorized electronic surveillance. While this simple service remains available at low cost to consumers, it is not adequate for business-level security. A corporate **Inspection Process** outline may be viewed here.[1]

Most people are unaware that:

- scheduled inspections became a standard business practice decades ago,
- they are usually conducted quarterly,
- and TSCM inspections, when conducted by a qualified external specialist, also provide valuable information security insights and recommendations.

These are three very important points management needs to know.

Benefits to Organizations

- Increased profitability.
- Intellectual property protection.
- An environment secure from electronic surveillance invasions.
- Advance warning of intelligence collection activities (spying).
- Double check the effectiveness of current security measures and practices.
- Shows compliance with many privacy law requirements.
- Discovery of new information loopholes *before* they can be abused.
- Helps fulfill fiduciary responsibilities to stockholders.
- Helps fulfill due diligence requirements.
- Establishes a limited window-of-vulnerability should an attack be discovered.
- Helps fulfill legal requirements for *"Business Secret"* status in court.

[1] https://counterespionage.com/tscm-inspection-process/

- Helps fulfill Wi-Fi network legal compliance:

-- Sarbanes-Oxley Act	-- HIPAA	-- ISO 27001
-- GLBA	-- PCI-DSS	-- Basel II Accord
-- FISMA	-- DoD 8100.2	-- EU - CRD

Benefits to Security Departments

- Zero capital investment in expensive and unprofitable instrumentation.
- No attendance at expensive *and* time-consuming training schools.
- No worries about maintaining TSCM skill sets.
- No risk to your department's reputation.
- An external consultant's recommendations can fortify and advance previously made recommendations.

When Management Asks

"Should we really be doing this?"

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

- ☑ Business Espionage
- ☑ Competitive Intelligence
- ☑ Mysterious Leaks
- ☑ Personal Privacy (including spycams in expectation-of-privacy areas)
- ☑ Internal Intrigue
- ☑ Strategy Spying
- ☑ Media Snooping
- ☑ Blackmail
- ☑ Revenge
- ☑ Eavesdropping
- ☑ Malignant Activism, Protests and Boycotts
- ☑ Adverse Publicity
- ☑ Embarrassing Photos

"What types of information should we be protecting?"

- ☑ Sensitive Communications
- ☑ Boardroom Discussions
- ☑ Merger & Acquisition Strategies
- ☑ Delicate Negotiations

- Lawsuit Strategies
- Employee Safety Measures
- Trade Secrets
- Personal Privacy
- Vulnerable Off-site Meetings
- Wireless Local Area Networks (Wi-Fi / WLANS)
- Executive Residences & Home Offices

"Do we legally need this type of security?"

Yes. Consider your obligations...

- *Fiduciary Responsibility* to stockholders.
- *Duty of Care* to protect trade secrets, intellectual property and strategic communications.
- *Due Diligence* requirements.
- To fulfill the legal requirements for *business secret* status in court.
- Wi-Fi network legal compliance.

Benefits of Scheduled TSCM inspections

- Increased profitability.
- Intellectual property protection.
- An environment secure from electronic surveillance invasions.
- Advance warning of intelligence collection activities (spying).
- Checks effectiveness of current security measures, policies, and practices.
- Documentation of your compliance with privacy laws.
- Discovery of new information loopholes ***before*** they are used against you.
- Help fulfill legal the requirements for *"Business Secret"* status in court.
- Enhanced employee personal privacy and security.
- Improved corporate growth and job security boost employee morale.
- If management cares about information security, employees will care. (and vice-versa)
- Wi-Fi Security and compliance with privacy laws.
- Increase employee respect for information security.
- Increase effectiveness of established security measures.
- Reduction of consequential losses from events such as…
  - An information leak which sparks a stockholder lawsuit.
  - Activists releasing wiretaps. paperwork or photos in an effort to blackmail, or damage reputation and sales.

“What should be part of a TSCM inspection?”

- Boardrooms
- Trading floors
- Executive suites
- Conference rooms
- Corporate apartments
- Quarterly Board meetings
- Vehicles, aircraft & yachts
- Off-site business meetings
- Family management offices
- Individual privacy protection
- Expectation of Privacy areas
- Wi-Fi systems & USB cables
- Counterespionage consulting
- Espionage vulnerability surveys
- Hotel rooms & conference centers
- Executive homes, offices & bunkers

"I agree, this is smart. What's the process?"

1. Plan a Strategy

- **Consult The Security Director's Guide to Planning an Effective TSCM Sweep**,[2] for assistance. Tell your **Technical Information Security Consultant** about your information security experiences, concerns, and goals.
- **Create a priority list** of the locations requiring a detailed inspection. Some inspection tests may cover the entire building, so not every space requires a detailed inspection. Focusing attention on the most sensitive areas provides better results, and keeps costs low. A floor map will help your consultant with planning.
- **Determine the proper frequency of follow-up inspections** — everyone's window-of-vulnerability is different. Most organizations find quarterly or biannual inspections suit their needs. Some use a mixture of both. Extra inspections for off-site meetings, Board meetings, and periods of elevated risk may always be scheduled, as needed.
- **Request a written proposal**.

2. Schedule Inspections

Arrange a mutually convenient time to conduct your inspection. TSCM bug sweep inspections may be scheduled any time, day or night. Your consultant should handle all the travel arrangements for you. You simply pick a time and date for them to arrive. Upon arrival, it is wise to review your concerns, goals, and discuss any late-breaking events. Do this out of any areas of concern, of course. This is also a good time to provide 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 inspections are conducted quite a bit differently.

Information (visual, audio and data) may be transferred from sensitive areas in a variety of ways. There is no "one" test or gadget which will detect every transmission method. To detect these possibilities your consultant will develop a customized inspection protocol augmented with their specialized instrumentation.

---

2 https://counterespionage.com/media/tscm-security-reports/security-directors-guide-plan/

Caution: Instrumentation is only a tool. The person using it is the key to effectiveness. Anyone can purchase instrumentation, so don't be dazzled by hardware. Your consultant's knowledge and experience are the most important elements for success.

3. Elements Common to Most Inspections

- **Radio Reconnaissance Spectrum Analysis** - a search for surveillance devices which transmit information via radio waves. Also included: Wi-Fi security and compliance evaluation, Bluetooth & GPS tracking devices, and some of the more obscure radio-frequency modulation types.
- **Thermal Emissions Spectrum Analysis** - detection of 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. Heat signatures can remain long after a hidden surveillance device has been remotely turned off.
- **Communications Systems Surveillance Analysis** - a group of tests which identify surveillance methods used to extract information from communications devices generally found in business environments.
- **Mapped Physical Inspection** - areas are systematically segmented for 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 on other security issues. This is the most important phase of the inspection, and relies heavily on security knowledge, experience, and intelligence.

Example: A clear thread seen in a drape or carpet may look normal. A qualified TSCM consultant would suspect it could be a fiber optic microphone... and search further.

- **Non Linear Junction Detection** - areas are re-examined using non-destructive radar. This safe technique reveals semiconductor electronic components (transistors, diodes, etc.), the building blocks of electronic surveillance devices. Devices hidden in - or built into - furniture, ceiling tiles, and other objects can be identified with this technology... even if they are not active during the inspection!

- **Additional tests...**
  Each of the basic inspection elements also contain sub-tests. Spectrum Analysis, for example, is not simply radio wave analysis. Light wave analysis is also conducted, as light can move sound too. In fact, there are several dozen individual sub-tests. Like other diagnostic crafts, e.g. the medical profession, TSCM techs craft inspections by selecting the appropriate tests for each situation.

"Will I receive a written report?"

Yes. Written reports should detail:

- locations inspected,
- findings,
- recommendations for remediation,
- non-electronic information security vulnerabilities noted (with recommendations for remediation),
- and explanations of the inspection methodology and instrumentation.

Most reports also will also include documentation photographs and an Annual Inspection Log. Your report should prepared by an independent and credentialed security consultant. The report is proof of your due diligence. The consultant should be qualified to testify in court as an expert witness, should that become necessary.

The advice given here will help you fill the gap in your overall protection program. Hopefully, your conversation with management will end with…

"Let's create an inspection schedule. What do we need to do?"

The easy answer. Call me.

More important, however, is that you actually institute an inspection strategy, and partner with a qualified TSCM specialist. There are several good ones to choose from, but remember, 9 out of 10 didn't graduate in the top 10% of their class. Check resumes[3] and comparison shop.[4] Background check.

Tip: The **International Association of Security Consultants**, **iapsc.org**,[5] is **the** resource for finding highly-qualified security consultants from all specialities.

---

[3] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-tscm/

[4] https://counterespionage.com/about-murray-associates/compare/

[5] https://iapsc.org

Until then…

General Guidance

Review your information security policies, especially the all-important **Recording in the Workplace Policy**. If you don't have one, click here.[6]

If you suspect you have an electronic surveillance problem…

- Do not discuss TSCM services in, or call a specialist from suspect areas.
- Conduct your affairs normally.
- Do not reveal any suspicions you may have to others.
- Limit confidential conversations.
- Keep detailed notes about anything you feel is suspicious.
- Think ahead. If a device is found, what next? Your Technical Information Security Consultant can advise you about the options.

"May I contact *you* with additional questions?"

Please do. Click here... https://counterespionage.com/contact-murray-associates-tscm/

———

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

Murray Associates 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.

[6] https://counterespionage.com/workplace-recording/