

M u r r a y A s s o c i a t e s



Murray Associates

**The Security Director's Guide
to Planning an
Effective TSCM Sweep**



Contents

Introduction to TSCM Planning	3
Creating a Strategy	4
Your Strategy Checklist	4
<input type="checkbox"/> Select a TSCM Consultant	4
<input type="checkbox"/> Create a List	4
<input type="checkbox"/> Prioritize your List	5
<input type="checkbox"/> Re-inspection Schedule	6
Make Your Strategy Cost-Effective	6
Schedule according to vulnerability levels.	6
<input type="checkbox"/> Obtain a Written Estimate	6
<input type="checkbox"/> Turn-Key Simplicity	7
<input type="checkbox"/> Now, sit back and relax...	7



Introduction to TSCM Planning

If **Technical Surveillance Countermeasures** (TSCM) is new to you, please review [The Security Director's Guide to Discussing TSCM with Management](https://counterespionage.com/media/tscm-security-reports/security-directors-guide/).¹

Successful TSCM inspections...

- Assure confidentiality,
- Protect sensitive information,
- Maintain competitive advantages and profitability,
- and, are cost-effective.

Key to accomplishing all this is a smart strategy, knowledgeable execution, and follow through.

The guidance here will make your planning easy *and* cost-effective.

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.

Linked in <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

¹ <https://counterespionage.com/media/tscm-security-reports/security-directors-guide/>



Creating a Strategy

The decision to conduct TSCM inspections usually evolves in one of two ways...

“How did that get out?! We must be bugged. Get the building swept.”

Let's stop. Take a breath. Think. This is a predictable first reaction, but sweeping the entire building, or floor, is not always the best solution. A thoughtful strategy provides the best solution, and cost-effectiveness.

“The other Board I sit on does TSCM sweeps. We should too.”

Taking corporate espionage seriously, and creating a strategy to prevent it, is cheap insurance. No, it's better than insurance. It can prevent the loss in the first place.

Your Strategy Checklist

Select a TSCM Consultant

This is the most important item on the checklist. A knowledgeable and experienced consultant will make creating a strategy easy. They will also make sure the plan is effective, and save you from costly mistakes. You may want to read, [How to Choose a Competent TSCM / Counterespionage Consultant](https://counterespionage.com/competent-tscm-consultant/),² before continuing.

Create a List

Include the most sensitive areas in your organization. These may be the: Boardroom, executive suite offices, vehicles, and departments like HR, Legal, R&D, and Marketing.

Include *all* sensitive locations when planning your technical information security strategy. Include remote facilities, and regional offices, for example. Do this at the outset and you will likely be offered an extensive / multiple operation discount. Doing it later risks continuing with the individual pricing unless *you ask* to re-negotiate.

Don't forget to include **expectation-of-privacy** areas: restrooms, locker rooms, gyms, changing rooms, etc. used by the public, employees, or invited guest to your premises. The amateur spycam epidemic is creating expensive lawsuits, and public relations

² <https://counterespionage.com/competent-tscm-consultant/>








nightmares. Alternately, you can **train**³ your security / facilities personnel to handle the inspections in-house.

Prioritize your List

Top of the list... areas where electronic surveillance would cause the most damage (competitive advantage, cost, reputation, loss of business, embarrassment, etc.). Concentrate your TSCM team's efforts in these areas.

Bonus... Surrounding areas, including the floors above and below, benefit from the radio-frequency and Wi-Fi security analysis by default, *at no extra charge*.

Bugs Live Here...

	<ul style="list-style-type: none">● Boardrooms● Trading floors
	<ul style="list-style-type: none">● Executive suites● Conference rooms● Corporate apartments
	<ul style="list-style-type: none">● Vehicles, aircraft & yachts● Quarterly Board Meetings
	<ul style="list-style-type: none">● Family management offices● Wi-Fi systems & USB cables● Expectation of Privacy areas
	<ul style="list-style-type: none">● Executive home offices & bunkers● Hotel rooms & conference centers

³ <https://counterespionage.com/what-is-tscm/spy-camera-detection/>



Re-inspection Schedule

Re-inspections are important. They limit the window-of-vulnerability and establish due diligence. If an eavesdropping device is found, any information loss is limited to a known time frame. Frequency may also be a factor in court when determining your “*trade secret*” status.

Make Your Strategy Cost-Effective

Schedule according to vulnerability levels.

- ▶ Schedule Board meetings, off-site meetings, and conference rooms used for visitor/vendor negotiations, on a per-event basis.
- ▶ Boardrooms, executive suites, IT closets, and vehicles may be safely assigned periodic schedules (e.g. monthly, quarterly, biannually), *if protected by other layers of security, and outside access is limited.*
- ▶ Active litigation events may require daily or weekly inspections.
- ▶ And, for executives who may not be as important as they think they are, once or twice per year is advised to keep egos from being bruised.

These are just suggestions based on years of experience. It is your call. Every organization is different, and priority lists will change with time.

Obtain a Written Estimate

In addition to a priority list your TSCM information security consultant will likely ask for: a floor map, the square footage of the areas involved, and will need to know if there are any special items, like audio-visual or other communications equipment to consider.

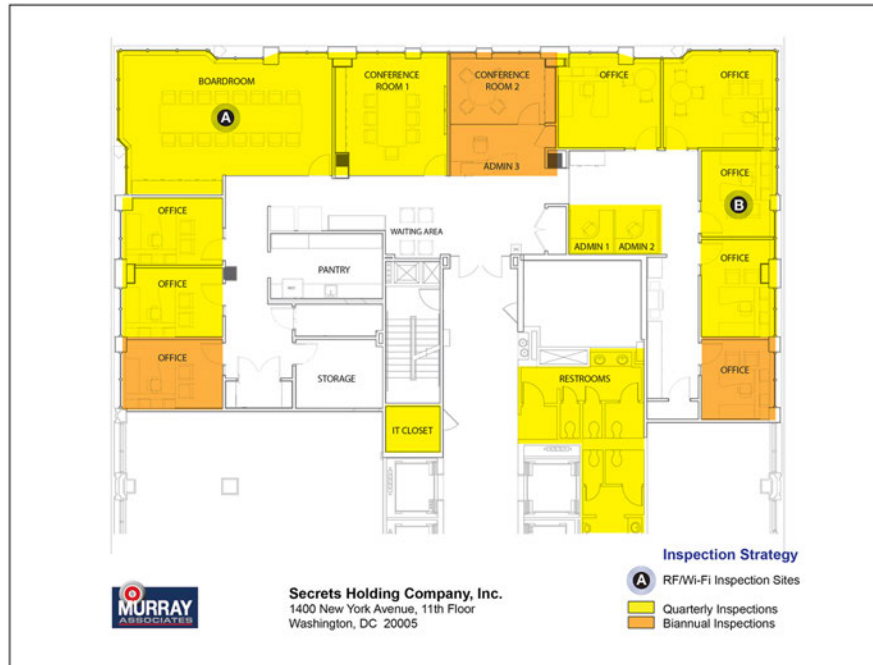
If pricing is based on floor measurements it should only include the square footage of areas requiring a detailed physical inspection. Hallways, utility areas (excepting IT areas) should not be included when determining cost. If this information is not easily available, square footage can be *estimated* from a floor map, and laser measured during the inspection.

Tip: An on-line form [like this one](https://counterespionage.com/estimate/)⁴ makes the estimate process easy.

⁴ <https://counterespionage.com/estimate/>



This floor map is the typical way an inspection strategy is graphically explained.



All areas, colored or otherwise, benefit from the radio-frequency / Wi-Fi analysis during every quarterly inspection.

☐ Turn-Key Simplicity

Your TSCM consultant will manage scheduling, travel arrangements, and re-inspection reminders for you. This is especially helpful with complicated, enterprise and international TSCM inspection schedules.

Be sure to tell them your *must-have* dates (Board meetings, special events, etc.). Plan every January for the whole year. Then, let your consultant suggest tentative dates for the periodic general inspections. Once these dates are mutually agreeable, they go on the calendar too.

Tip: If another one of your consultant's clients has an emergency it may create a scheduling conflict. Allow them to reschedule your non-emergency inspection date. In return, when you have an emergency, you will receive the same priority treatment. The chances of this happening are very rare. However, having this understanding in place puts everyone at ease.

☐ Now, sit back and relax...

You have this important element of your security covered.



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, CDPSE



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