CHARTSEC

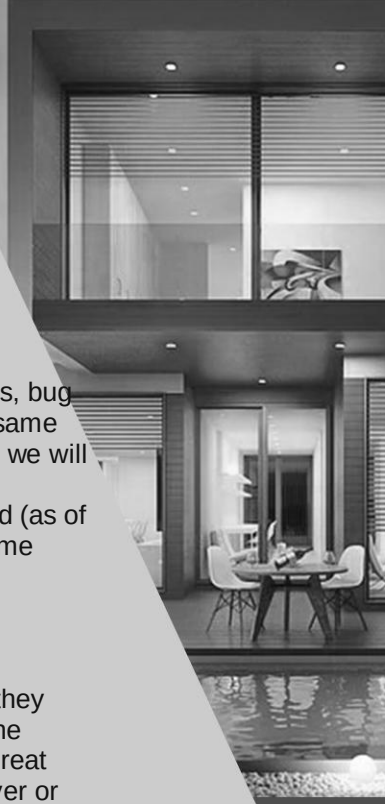
CHARTERED SECURITY SERVICES LIMITED

TSCM Technical Surveillance Counter Measures

GUIDE TO TSCM SWEEPS:

Office Numbers: 0161-262 2456 alt: 262001
Director Security: Des Steel -079600 03323 – Alt: 077895 40663
Director Business Development: David Hesketh – 07395 535575

Web: www.chartsecservices.co.uk
Email: services@chartsecservices.co.uk



GLOSSARY INFORMATION:

TSCM Sweeps:
Technical surveillance counter measures or **TSCM** sweeps are known by many different names, bug sweeping, TSCM Inspections or electronic counter-surveillance etc. really, they are all one in the same thing, an electronic and physical check or inspection of a room, building, area or vehicle. For ease we will refer to these services as a TSCM Sweep.
In this guide we cut though the technical speak and look at some of the latest equipment employed (as of June 2015), what a TSCM Sweep should include, look at present and future threats and dispel some myths surrounding eavesdropping.

When should a TSCM sweep take place?
Ideally companies should look at TSCM sweeps being part of their security housekeeping policy; they should have a security and risk policy that includes the budgeting for TSCM. The frequency and the requirements are very much down to the individual company and how they perceive the level of threat against them at that particular time. For instance a company might be involved in a hostile take-over or substantial litigation and may wish to increase the level of service at that particular time.

If a company feels that it may have an issue of loss of sensitive information then a TSCM sweep is not the only thing that it should be thinking about. This is very much a common mistake and one that is very much regretted in hindsight.
Should a company find that it is in the position where it feels it is losing information or data then really that company should launch a full internal investigation and where were required call in external counter espionage experts.

In many cases the loss of sensitive company information can be down to failing in internal policy, such as office refuge, key staff leaving. It's not always about targeted acts of espionage, but if this is the case, it's often worthwhile managing the issue correctly leaving options of legal action. Should this be miss-managed at an early stage then it is difficult to regain the situation and opportunities to gather key evidence may be lost.

A little about eavesdropping devices:
Just to dispel a few myths and misinformation about "bugs" or covert transmitters for a moment before we go into more detail about countering these threats.
Most people's understanding of bugging or eavesdropping devices comes from watching television, films or popular fiction books such as of course the legendary James Bond or the good shepherd, staring Matt Damon. This is not the 1980's and the Cold War, times and technology has moved on leaps and bounds; that is not to say that some espionage technique developed then is still not applicable today.

Those who plant covert bugging devices need to look at lots of options before even getting to the stage of entering the building/area and planting any devices.
Considerations could be and are not limited to:

- Cost vs reward.
- Level of risk.
- Type of building (Steal & concreate or brick).
- Location of target room/area within building.
- Timescale monitoring/eavesdropping is required.
- Monitoring or receiving location.
- Access to room/area and building.

The above gives just a small insight into the questions that need to be asked before even selecting what type of device to deploy, UHF, VHF or GSM etc. That is even before you get onto how the device is going to be powered or how and where the signal is going to be received.

It would be very foolish to think that you could just buy a device, plant it and place it within an office; there is much more to it than that, many more things to think about, not to say of course that a person with no prior knowledge or training could not pose a threat.
If a device is not tested once in place, then how will you know that it is going to work as desired?

Can it pick up audio ok; is there too much background noise? is it transmitting correctly? These are all further questions. With GSM devices, does the chosen network operate with high signal strength in that building is one big technical consideration and further questions for those carrying out acts of industrial or corporate espionage.
Small eavesdropping devices are great for quick short-term task such as those built into pens, computer mice or stuck under desks or chairs etc. But devices have their drawbacks and devices that are going to be required to be in position long term require more sustainable power supplies and are normally “hard wired” or built in to powered devices; for example plug sockets, extension leads, phones or computer monitors etc.

“Sometimes it really is as simple as placing a Dictaphone on voice activation for later retrieval.”

Since the mid 2000's and the rise of internet usage there has been a large increase in “off the shelf” eavesdropping devices, these range from complex GSM devices to the lower end of the scale FM, UHF devices. But one thing for sure, £100 can buy you a reasonable device capable of causing a company loss of vital commercial information; i.e. Damage and loss of profits.

An individual or organisation carrying out acts of espionage is going to look at the easy options for intelligence gathering first, the easiest with the least risk and the most cost effective. Eavesdropping and monitoring of devices is expensive and full of risks with huge damaging to profits and reputations if caught; not forgetting prison sentences. That said very few corporate espionage cases are ever brought to court, victims instead prefer to settle such matters outside of court to save bad PR and reputational damage.

Present and future espionage threats:

The last fifteen years eavesdropping devices have got smaller and smaller as surface mount technology has got cheaper; batteries too have become more stable and of course smaller.
£500 will now by you a GSM double plug socket transmitter; capable of being in situ for many years and monitored anywhere in the world.
The only saving grace with GSM devices is that due to the terror attacks of Al Qaeda and timed or sequenced Improvised Explosive Devices (IED's) SIM Cards that are unregistered have become harder to purchase in many western countries. So at least SIM Cards is becoming more attributable.

Those designing bugging devices have become more intelligent with an emphasis on burying the device within a functioning electronic device, such as a monitor. These devices normally GSM transmitters are hard-wired and almost impossible to find.
What is the future of bugging or eavesdropping devices? I think that the high end of the market will see more intelligent devices that will be harder and harder to detect, programmable to sleep with masked heat signature and they will of course keep getting smaller.

The lower end of the market keeps growing with cheaper electronic devices almost a novelty. A quick internet search for “bugging device” will demonstrate the vast variety of website offering cheap yet functioning eavesdropping devices.

“It's not about how expensive the bugging device or how experienced the user, it's about the potential damaged caused”

TSCM Teams:
A professional TSCM service provider should be able to provide you with a full team of operatives each bringing a different skill set or range of qualifications. If your TSCM firm arrives and it's one bloke with a few pieces of equipment; then you have made the wrong choices.

A TSCM team should comprise of a Team Leader from a solid intelligence or military intelligence background with an understanding of present technology and threats. Ideally (dependent on the size of the task) a sweep team should comprise of a qualified electrician (to check electrics, ducting, fitting and sockets) and also a qualified telecommunications engineer to check telephone lines to the point where the lines enter the building. Team can consist of plus **+1-2/3** individuals.

How should a TSCM sweep take place?
Exactly how a TSCM Sweep takes place is very much dependent on the topography of the building and how it is laid out, how many floors, open office space etc.
Ideally going into the target building at night when there are no workers in the building, normally the TSCM Team would set up in a central location on each individual floor that requires sweeping (in the case of a rural residence, one location is suffice).

TSCM Equipment:
A TSCM Team should employ different TSCM equipment, each piece of equipment carrying out a specific role. As standard you would expect any TSCM firm worth its salt to be using a spectrum analyzer such as the OSCOR Green, a state-of-the-art electronic counter measures receiver sweeping from 10 kHz to 24GHz in seconds. The purpose of the OSCOR Green is to survey the given area and produce a spectrogram of receiver traces; i.e. it maps all the frequencies transmitting (between 10 kHz to 24GHz) in that given area. Based on this survey an operative can then go about analyzing the results looking for possible suspicious transmissions, ruling out "normal" background traffic.

Over and above a spectrum analyzer survey a team should also be looking for redundant, hardwired devices, covertly placed recording devices (such as Dictaphones) or devices that are piggybacking on or off the back of genuine electronic devices (such as telephone lines or computers). To look for these devices both a physical and technical inspection is required; often employing equipment such as a Non-Linear Junction Detector. This looks for and detects circuitry used within circuit boards or microphones that are or are not powered at that time, i.e. "Passive devices".

There are many, many other types of equipment that can and should be deployed on a TSCM Sweep; from Thermal imaging cameras to look for hear signatures of devices buried within walls or soft furnishings to GSM specific devices such as SEARCHLIGHT. This is a dedicated GSM/UMTS detection and location system, designed to identify the IMEI of the SIM card and can quickly distinguish between legitimate or authorised mobile phones and GSM bugging devices transmitting within the given target area.
"It would not be an underestimate to expect a firm offering TSCM sweeps to have invested well in excess of £50,000"•

What should be inspected?
One basic schoolboy error by large companies is forgetting common areas, toilets, lifts and refreshment areas. Often these areas are where sensitive conversations take place and these areas should not be ignored.
Meeting rooms and offices of Directors or senior partners should be at the very top of the list, not forgetting of course offices of related Personal Assistants. Open areas are in many ways harder to sweep with a number of sockets and work stations. These areas take time and particular attention should be paid to allotting the correct amount of time to the task.

A physical inspection of all sockets, ducting, lighting and electronic devices should be conducted by a qualified electrician, someone who is of course knowledgeable and well versed when it comes to eavesdropping devices.

Great care and attention should be paid to the telephone system within the building. A qualified telecommunications engineer, again with knowledge of eavesdropping devices, should inspect this. Telephones systems are an easy option when it comes to espionage, and a conferencing system or desk telephone can be so easily turned into a listening device, quickly, just by tampering with the device and wiring. It is very, very simple and almost impossible to detect unless you have specialist and up to date knowledge of telephone systems.

Vehicles are often inspected, not just cars, but also private yachts and aircraft as subject to being swept. Each of these vehicles poses a different set of problems and approaches and requires expert knowledge not only of eavesdropping devices and capability, but of the wiring and workings of those vehicles. A TSCM sweep on a car takes a great deal of time and involves endoscopes and thermal imaging devices and of course a knowledge of what is and what is not possible when it comes to deploying eavesdropping devices.

Are Computers normally covered as part of a TSCM inspection?
Not normally covered on TSCM sweeps computers can also be turned into eavesdropping devices just with the edition of spyware, not a real worry for large companies with IT Security managers and teams, but totally forgotten and overlooked when it comes to Company Directors working remotely from home. A qualified IT expert should physically inspect computers. Very few TSCM firms cover computers during TSCM Sweeps, even though computer cases are the ideal place to conceal a hard-wired device.

The lack of technical knowledge being one issue; a member of a TSCM team might not know what he/she is looking at/for within the circuits of a computer. Another reason is because most senior management would expect the IT department to know what is inside each workstation computer and that it is their responsibility.
I very much doubt that an average IT expert would notice another small circuit or card or more wiring within a PC.

Further information:
A TSCM Sweep should be part of your ongoing security and counter espionage policy; employed alone in isolation they are a token gesture.
Should you require more information about Technical Surveillance Counter Measures or counter espionage services, please do get in contact with us. All enquiries are treated with the utmost confidentiality and of course we would encourage the signing of a confidentiality or non-disclosure agreement when discussing issues or problems that you might be facing.
International Intelligence Limited TSCM Sweep service information page can be found here:
A latest equipment list that our TSCM teams use can be found here:

TSCM EQUIPMENT:
International Intelligence Limited use the very latest in military grade TSCM equipment. The TSCM equipment selected will be dependent upon the Country location, the size and complexity of the inspection.

- **Oscor Green:**
The Oscor Green is a hand-held spectrum analyzer with a rapid sweep speed and easy to use functionality suited for detecting unknown, illegal, disruptive, and anomalous rogue transmissions across a wide frequency range.

- **Spectrum ECM6:**
Comprising a purpose-built Spectrum Processor linked to a lap top computer with full video display capability. The equipment gives full USB, LSB, CW, FSK, AM, FM and WBFM coverage with Video Display capabilities. Frequency ranges 10 KHz to 6 GHz.

- **Merlin RF Receiver:**
Comprising a purpose-built Radio Spectrum Processor linked to a lap top computer. RF modes covered are similar to Spectrum ECM6 Frequency ranged covered to 3 GHz.

- **Searchlight:**
A GSM/UMTS detection and location system. The equipment is designed to detect any active SIM based surveillance devices across all service providers. The equipment will also detect tracking units hidden in clothing, personal items, vehicles, boats etc.

- **Talan:**
The Talan is a telephone and wiring analyser which detects eavesdropping devices on analogue or digital telephone lines. The equipment has a built in Frequency Domain Reflectometer (FDR) which

measures cable lengths and detects unauthorized junctions. The TALAN also identifies all telephone pair combinations.

- **CPM 700 Counter Surveillance Probe/Monitor:**

This equipment detects and locates all major categories of electronic surveillance, including room, phone or body bugs that are transmitting conversations. RF spectrum to 12 GHz.

- **Locator XDi Non-Linear Junction Detector:**

This equipment is designed to detect passive eavesdropping electronic surveillance devices, either hardwired or remotely controlled using Third Harmonic technology.

- **Bloodhound:**

Fully portable Acoustically Stimulated Microphone Detection System. This equipment detects amplified wired microphone systems where the target site is wired directly to a listening post. It operates by detecting the audio signal from a microphone and subjecting it to high amplification with elaborate filtering to remove extraneous noise.

- **Hunter XD Radio Microphone Detector:**

This equipment detects clandestine radio microphones including “smart” bugs such as frequency hopping and spread spectrum.

- **High Specification Search Kit:**

Including a range of cable testers, specialist search tools, UV lights and digital camera equipment etc

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) FREQUENTLY ASKED QUESTIONS:

What does Technical Surveillance Counter Measures (TSCM) mean?
A Technical Surveillance Counter Measure (TSCM) sweep is also commonly referred to as an Electronic Bug Sweep or an Electronic Surveillance Sweep. A TSCM survey is a service provided by qualified personnel to detect the presence of technical surveillance devices (eavesdropping or spying devices) and other information security hazards and to identify technical and communications security weaknesses that could aid in the technical penetration of the surveyed facility.

What is the definition of Counter Surveillance?
Counter surveillance refers to measures taken to prevent or disrupt surveillance, including measures to prevent electronic eavesdropping. Counter surveillance may include electronic methods such as TSCM "bug" sweeping, the process of detecting surveillance devices, including covert listening devices and visual surveillance devices (video). More often than not, counter surveillance will employ a set of actions (countermeasures) that, when followed, reduce the risk of effective surveillance.

Who is a target of eavesdropping or spying?
Companies, law firms, non-profit entities and charities, governments, private individuals, no one is immune from spying. The bottom line is, if you discuss valuable information that would be of benefit to anyone, be they a business competitor, opponent in a lawsuit or some other adversary, then you are a potential target of electronic eavesdropping.

What are some indicators or "warning signs" that you are the subject of spying?

- You recently lost a Bid or Request for Proposal that you would normally win
- You have an unexplained decrease in new sales
- Your company's business strategies are revealed
- Your pricing and sales strategy is known by your competitors
- Contract negotiations for labour and contracts are more increasing more difficult
- Company trade secrets are exposed

If any of the above has occurred, you should consider revisiting your risk management protocols and consider scheduled Technical Surveillance Counter Measure sweeps.

What are some high threat business situations?
Anyone can be the target of covert eavesdropping and spying however; some companies or organizations are at higher risk than others because of their occupation, financial position or legal situation. A company is most in danger of an electronic eavesdropping attack when:

- Business expansion or reorganization plans are being discussed
- Key executive(s) leave or are leaving
- New products, pricing or marketing plans are being developed
- Acquisitions or mergers are being planned.
- It is in a sensitive or high-profile industry
- Executives or clients are subject to media attention.
- There are ongoing labour negotiations, labour problems or union activities
- It is involved in any type of litigation, lawsuit, or other civil action

Where are you likely to be targeted?
The Company boardroom, telephone system, mobile phones, fax machines, computers are examples of sources of confidential information that may be targets for the eavesdropper. Also, eavesdropping need not be confined to the company office. Executives and other key personnel can be targets at home or in their automobiles.

What are typical environments where a listening device would be hidden?

- Business Offices, including conference rooms, boardrooms and trading floors
- Private Residences
- Executive Residences
- Corporate Apartments
- Vehicles (Cars, Aircraft, Boats)
- Cell Phones
- Home Phones (landlines)
- Quarterly Board meetings
- Off-site business meetings

Any area in which important information, that would be valuable to a third party, would be openly discussed with other persons present or via a telecommunication device present in that area, which has not previously been rendered secure.

What types of devices will you screen for during the sweep?
There are many types of electronic eavesdropping devices or bugs. During an MSA Investigations TSCM sweep, we will typically search for the following devices:

- Micro wireless video devices.
- Laser and infrared eavesdropping devices.
- RF, UHF and VHF wireless transmitters.
- Wire and microphone taps.
- Telephone taps.
- Carrier current devices.

Where can bugs be hidden?
Electronic eavesdropping devices (bugs) can be hidden in any room, device, furnishing or container that would typically be found in an office or home setting. Today's eavesdropping devices are smaller, more sophisticated, less expensive and easier to hide than they have ever been. Video as well as audio can be captured, recorded or even transmitted live. The good news is that all of these devices are detectable with the right people, equipment and methodology. It is also left to the imagination of the individual and technical skill set to the people undertaking the eavesdropping, combined with the financial and technical resources at their disposal.

What happens during a typical TSCM Investigations, examination?
Our TSCM professionals will conduct a detailed examination of your location in order to:

- Discretely determine the threat to the location.
- Detect the presence of technical surveillance devices and hazards.
- Identify technical weaknesses that may allow illegal penetration of your facility.
- Provide a professional evaluation of your facility's technical security position.

During the actual sweep, our team will visit the location of concern and perform a comprehensive visual, physical, and electronic inspection to determine the presence and location of any and all electronic eavesdropping devices. We will also identify other technical weaknesses that may exist in your security posture.
During visual inspections, we look for hidden eavesdropping devices in areas in which they are commonly found.

During physical inspections, we take it a step further, physically and thoroughly examining furniture, outlet covers, ceilings, and other locations commonly housing hidden eavesdropping devices such as microphones, recording devices, transmitters, camera systems, and more. During the electronic inspection we use a variety of sophisticated electronic equipment to identify and locate hostile signals and other tell-tale signs from eavesdropping equipment that may be secreted in the area. Additionally, we survey AC electrical outlets, telephone cables, computer lines, and other wiring capable of transmitting communication, looking for wiretapping and other intercept devices.

After all TSCM sweeps, the provision to provide you with a detailed written report, or verbal account of the results examination and any recommendations on improving your technical security posture. Should any follow-up measures be needed (e.g. the removal of a recording device), we will work with you to identify the origin of the device and help put measures in place to reduce future risk of attack.

How long does it take for a TSCM sweep to be conducted?
TSCM Sweeps can take anywhere from a few hours, to a few days and in some cases as long as a couple of weeks. It depends on the size of the area or building to be swept, and the amount of electronic and communications present within the concerned area.

What does a Legitimate Bug Sweep Cost?
Electronic eavesdropping detection is a highly specialized and professional field. It requires an array of sophisticated and expensive hardware equipment and specialized software. Additionally, it requires years of practical experience and ongoing training to master the craft and to remain current in the field. It is not a service that can be effectively provided at a discount. The fees for our services are fair and consistent with the skill of our technicians and the value of the comprehensive TSCM sweep that we provide. It is also consistent with the industry pricing for a sweep conducted by a legitimate professional TSCM provider.

You should be prepared, as an minimum estimate, to invest between **£4,500** and £**6,500** for a typical, "small" one-day TSCM sweep. This will be dependent upon the size of the building and equipment to be used. Sometimes smaller, less comprehensive TSCM sweeps can be accomplished at a lower cost in some low threat situations only. The pricing for these TSCM sweeps is on a **case-by-case basis.** These figures above are exclusive of the cost for the hire and paid day rate for the technical team members. This excludes requirements to conduct initial surveys and confirmatory requirements, to provide accurate concise cost to the client. Obviously the larger the building and equipment's to be scanned the more costly the technical sweep.
Recurring scheduled inspections tend to be more cost effective and offer the best value, as we will establish a baseline friendly RF signal list during the initial TSCM sweep and build on this history during each recurring TSCM sweep. This signal history can then be used during each recurring sweep and will save the technician's time and therefore the client money. It will also allow for a more effective TSCM sweep.

Further Questions asked:

Additional TSCM bug sweeps cost?"

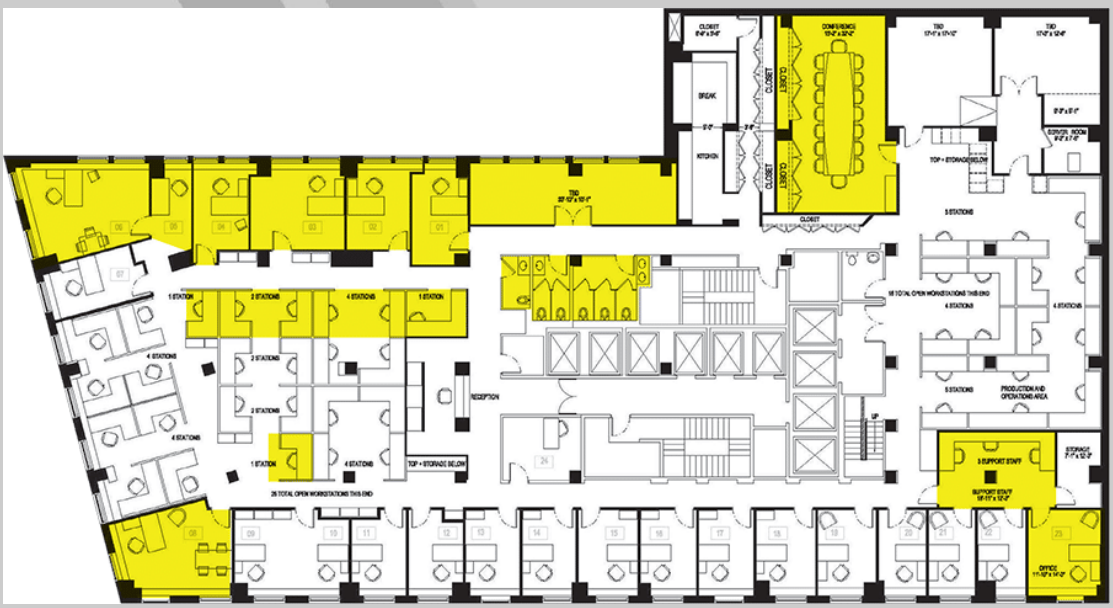
The cost of a Technical Surveillance Countermeasures (TSCM) bug sweep will depend on the type and category of the inspection. There are basically two types of bug sweeps,

- **Personal** -Home residence
- **Commercial** - Business (Higher cost implications due to complexities of equipment's and size of areas

Tip: Even the largest estates usually have less than 3-5 thousand square feet of sensitive areas that require a detailed inspection. So, paying for more square footage is rarely necessary, but could be a request form the client. Then the cost impact for whole rooms within a building is broken down into actual metres square.

Commercial TSCM Costs
Professional commercial TSCM bug sweep costs are usually estimated on a custom basis. Items considered include:
The square footage of sensitive areas which require a detailed physical inspection. If the inspection covers the whole office floor, do not use the square footage shown on the lease. Measure the sensitive areas individually.

Bonus: The radio-frequency / Wi-Fi analysis will cover the rest of the area by default anyway.



Example of a TSCM Bug Sweep Floor Plan

The number and type of communications items, within the sensitive areas (or within earshot of), requiring a detailed inspection. This would normally include: telephones, speakerphones, teleconferencing equipment, audio-visual racks of equipment, etc. Specify if you also want to have difficult to inspect items in the area X-Rayed. Although this will cost extra, it only needs to be done once. X-rayed items are tagged with discrete, tamper-proof security seals to identify them as already inspected during future re-inspections.

- Are the rooms / areas contiguous (having shared walls).
- Travel expenses.
- Special TSCM Bug Sweep Situations
  Inspection of: construction / renovation projects, data centres, off-site meeting locations, Transportation costs, special events, etc.

Tip: Obtain a line-item written estimate in advance, and never accept a per-hour based fee. You won't be able to control the cost.

From our experience, corporations budgeting estimate between **£30,000** and **£50,000** per quarter are providing themselves with adequate, pro-active, TSCM coverage at their headquarters locations.

"Why should we have a TSCM inspection?"

Crucially, regular scheduled TSCM inspections can help to keep your organization's confidential data safe and private, all while preserving your company's reputation. Electronic surveillance detection can help you avoid:

- Business Espionage
- Competitive Intelligence
- Mysterious Leaks
- Personal Privacy (including spy-cams in expectation of privacy areas)
- Malignant Activism
- Internal Intrigue
- Strategy Spying
- Media Snooping
- Blackmail
- Revenge
- Eavesdropping Concerns
- Adverse Publicity

"What do schedule TSCM inspections protect?"

- Sensitive Communications
- Boardroom Discussions
- Mergers & Acquisitions
- Delicate Negotiations
- Lawsuit Strategies
- Employee Safety
- Trade Secrets
- Personal Privacy
- Vulnerable Off-site Meetings
- Wireless Local Area Networks (WLANS
- Executive Residences & Home Offices
- Executive transportation (vehicles, aircraft)

Direct Benefits of Scheduled TSCM Inspections

There are many reasons why you should consider regular TSCM investigations, but the main benefits include:

- Increased profitability
- Intellectual property protection
- An environment secure from long-term electronic surveillance invasions
- Advance warning of intelligence collection activities (spying)
- Confirmation of the effectiveness of current security measures and practices
- Privacy law compliance
- Discovery of new information loopholes before they can be used against you
- Compliance with the legal requirement for “Business Secret” status in court
- Enhanced personal privacy and security
- Improved employee morale
- Wi-Fi security and privacy law compliance
- Increased employee respect for information security
- Increased effectiveness of established security measures
- Reduction of consequential losses, e.g. an information leak sparks a stockholder’s lawsuit, or…an activist releases wiretaps to damage good-will and sales

“TSCM inspection is a good idea. How do we start?”

Your TSCM investigator can help you plan your inspection, but here are some tips for starting. Plan a strategy.

- Define your security experience, concerns, and goals.
- Create a priority list of the locations requiring a detailed TSCM inspection. Even though some tests may cover the entire building, not every space requires a detailed inspection. Focusing attention on critical areas provides better results, and reduces costs.
- Determine the proper frequency of follow-up scheduled TSCM inspections — everyone’s window-of-vulnerability is different. Most organizations find quarterly or biannual inspections suit their needs. Some use a mixture of both.
- Schedule supplementary inspections, as required, for: off-site meetings, Board meetings, and situations where risks are elevated.

We will prepare a cost applied written proposal for you based on the information you provide. Upon deciding to have us help you, here is how it works:

Your Scheduled TSCM Inspection

Together, we arrange a mutually convenient time to conduct your TSCM investigation. Our services are available any time, any day or night. If required, we handle all the travel arrangements. Simply pick a time and date and we will be there.

Upon arrival, we will both define and refine your concerns, goals and any late-breaking events. This is when we ask for you to give us an orientation tour of your facility where we will look for vulnerabilities you may have overlooked.

Each TSCM inspection unfolds differently. Information (visual, audio and data) can be transferred from sensitive areas in a variety of ways. There is no “one” test, technique, or gadget which will detect every method. We have developed custom protocols, aided by specialized instrumentation, which we modify to fit your explicit organization’s security needs.

Elements Common to Most TSCM Inspections:

• **Radio Reconnaissance Spectrum Analysis:** A search for illegal surveillance devices which transmit (audio, video or data) information via radio waves.

• **Thermal Emissions Spectrum Analysis:** – Detection of heat emitted by spy-cams, bugs and other electronic circuits. Heat signatures can be found even when the devices are hidden in ceiling tiles, walls, or furniture.
• **Communications System Surveillance Analysis:** – a proprietary test method developed by Murray Associates – which identifies surveillance methods used to extract information from: telephones, faxes, computer networks, etc. In addition to inspecting the actual equipment (phones, speakerphones, faxes, video teleconferencing systems, etc.), wireless networks, LANs, and networked printers are also inspected. We also examine your wiring for taps and transmitters.

• **Wi-Fi Security Audits with Compliance Analysis:** – This is an examination of how the wireless network security is configured. This is important because it only takes one loophole for hackers to get in and your data to get out. Lack of proper network security can also create compliance issues; fines are very expensive.

• **Malicious USB Spy Cable Inspection:** – A malicious cable is any cable (electrical or optical) which performs an unexpected, and unwanted function. The most common malicious capabilities are found in USB cables. Data exfiltration, GPS tracking, and audio eavesdropping are the primary malicious functions.

• **Mapped Physical Inspection™** – Areas are systematically mapped for *physical inspection*. Each area is combed with several objectives in mind:

- physical penetration evaluation of the premises;
- location of hidden surveillance devices;
- discovery of evidence indicating prior installations;
- alerting you to future surveillance possibilities;
- reporting on other security and safety issues encountered.

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. Our technical investigators may suspect a fibre 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!

“Will I receive a written report?”

Yes. Your written TSCM inspection report will detail:

- locations inspected,
- findings,
- recommendations for remediation,
- non-electronic information security vulnerabilities seen – with recommendations, and explanations of our inspection methodology and instrumentation.

WHAT HAPPENS IF WE FIND BUGGING EQUIPMENT?

If our team discover bugging equipment or spy software in your home, office or vehicle, the following procedure is taken:

- Firstly, photographic evidence is taken.
- At least one of the device in its found location and at least one closer up.
- A note is taken of exactly where in the device/ equipment was found for the purpose of the report.
- A label is filled out and the device is numbered and put into an evidence bag. This is usually given back to the client to do with as you wish. Typically speaking, it will be used for an internal investigation if you are a corporate client or to the police for a criminal investigation.
- All information is compiled into a report which will support any potential proceedings

CHARTSEC SERVICS LTD (TSCM) TEAM PROFESSIONALS

Senior lead operative: TSCM

1. **Membership of professional bodies:**

Technical Surveillance Counter Measures Institute

2. **Other skills**:

- Surveillance Operator
- Anti and Counter Surveillance Trainer
- Experienced Covert entry operator
- Specialist in technical surveillance equipment installation
- Locksmith trained
- Technical Surveillance Counter Measures (TSCM)

3. **Years of professional experience:** 35 years

4. **Key qualifications:**

An experienced operator with a unique set of skills attained through over 30 years working with police, military and UK Government law enforcement agencies in the Counter Terrorism (CT), Counter Espionage (CE) and Serious Crime areas as both practitioner and manager.

Vast experience in technical surveillance (pro-active and defensive) with specialist knowledge in eavesdropping, CCTV, ground sensors, electronic countermeasures and technical surveillance sweeping.

Experienced in taking on complex security problems and producing secure non-technical and technical solutions. Produced and delivered written and oral briefings for, and to, senior officials and UK Government Ministers.

Experienced training officer who has devised, implemented and instructed on courses regularly for over 30 years.

Engaged from 2010 to 2016 as an Expert on EU funded law enforcement projects. Devised and delivered technical surveillance courses under the project in the Balkans for police and prison authorities. Also undertaken security reviews of offices and other locations for individual witness protection units.

DEPLOYMENT TASK: (COVERT TSCM TEAM)

Request for Coverts TSCM sweep,
Cyber Security and Communications Review.

Security Sweep
Premises and vehicle electronic and physical sweep – heat/radiation/electronic footprint/reflection & Physical search. Cutting edge equipment used. Profile of check on kit available.

TSCM Survey Aide Memoire

Confidentiality statement:

- We respect privacy at all times. No unnecessary intrusion unless a sound reason and only then by consent.
- We expect the same respect in our methodology and working practices.

Search limitations and privacy/human rights:
Personal areas (clothes lockers etc) not searched unless a good reason and only then by consent.

Requirement information requests:

- Intelligence Case.
- Threat (who, motive, access).
- Type of threat (opportunist, deep plant (i.e. State sponsored), remote (through or from adjoining properties).
- Skill level of threat if known.
- Access to premises (Building Management Services,
- visitors).
- Unusual events, visitors or business compromise.
- Floor plan.
- Priority rooms.
- Advance reconnaissance of residence.
- Op plan if devices found.
- Control of staff with access to search areas.
- Garage – vehicle search.

Planning:

- Team composition - 3
- Cover story -tbs
- Dress – as appropriate and as cover story
- Equipment – many large cases with specialist equipment
- Timings -tbc

Operational Plan:

- Operational location near to client consists of hotel and or apartment
- Entry to target – with equipment- (covert as required) blind into daily activities -night time alternative entry>
- Action on target (admin area, video, search)
    - need to have a designated area to set up. Commence with photographing the rooms before technical sweep followed by a covert search.
- Exit

NB. We work to covert standards to ensure that each area is left as it is found eliminating the chances of our work being detected by other.

Action on:

- Finding a device - options are leave in situ, neutralise or extract.
- Damage to property – minor damage, repair by team. Serious damage, covered by insurance
- Possible compromise – nominated backstop/person on site to advise
- Actual compromise – deploy cover story and inform nominated backstop

Post deployment:

- Report including recommendations and any follow up action
- Intelligence on any find
- Legal issues – We work to evidential standards in the UK

Cost Implications: are based upon first initial survey and findings evaluations for task requirements

- Initial survey & findings-recommended course of action plan
- Daily rate for a team of x3 experts
- Equipment hire
- Applied TSCM per property -vehicle-boat-plane
- Admin and support requirements
- Applied VAT

Chartsec Services Ltd:

Technical Surveillance Countermeasures (TSCM) Delivery Services:

"De-Bugging".

Corporate Operational Search Level-1 includes:

- Full spectrum RF search (Anything that Transmits) 0-30 GHZ.
- Full Wi-Fi penetration and analysis, access points and Routers LAN/ WAN.
- Full sweep of location walls, ceiling to floor, with electronic broom (NLJD) thermal Imager.
- Land line Telephone search, and networked systems, (Ethernet Connected Systems)
- All electrical systems on site removal of wall plates and sockets.
- GSM, mobile phone equipment search and penetration.
- Electronic Paint and Sweep, using digital scout equipment.
- Vehicle and GSM handset inspection and search are at the client's request, very bespoke.
- Infra-red and thermal search for laser microphones.
- GSM blocking and denial of service, jamming while survey is carried out.
- Full and complete technical inspection of all services entering the location or site.
- Surface or sub-surface technical inspection (IR Probes and CCTV).

A technical report will be compiled covering the various elements of the TSCM search.
If any devices are discovered on site, a specific technical profile will be compiled for the "Find"
All at the clients approval, either a corporate or government attack!
This level of counter measures can be added to, when specific threats are disclosed by the client.
Any after action involvement or other agency cooperation is at the client or principles request

CHARTSEC SERVICS LTD (COUNTER SURVEILLANCE) TEAM PROFESSIONALS

Mr. G.

- British Army 26 years Regular and Reserve (rank on leaving Captain SASC)
- Covert intelligence operator/ Team Leader Trainer
- Covert Surveillance Specialist Trainer
- Technical attack covert video audio operator Trainer
- Covert method of entry (level -1)
- Covert reconnaissance specialist Advanced trainer
- Weapons specialist Sniper Instructor
- British Army RMQ 1-3 Flat Ranges 4-5 Field Firing Ranges
- MTQ instructor and trainer
- Mountain warfare leader JSMEL Winter
- WO2 Specialized training team chief instructor tactics and ranges
- Specialist services for corporate clients
- Very advanced TSCM Government level services
- Corporate Counter Intelligence
- Covert advanced Intelligence gathering
- Electronic Personal Protection
- Counter kidnap and Ransom
- Counter Terrorism
- Counter Terrorism Covert Intelligence Services
- Asset Recovery/ Tracking

Personal statement:
I spent 12 years working for a PMC company which was owned by an ex-member of 14 Int, we specialized in providing technical and training support to UK Government and Police forces throughout the UK and Globally.

All forms of Technical Attack were carried out to Special Forces SF standards, money was no object in procuring kit and equipment as you will see when Chartsec Services Ltd undertake client presentations at their requests?

My target audiences are ex members of the UKSF, these people are of the same mind set of “Precision” and a no-nonsense approach, get the job done ! I don’t deliver a service I deliver Results. The devil is in the detail.

A former civilian Team Manager of the Ministry of Defence / Home Office looking to capitalise on my Investigative, operational planning, team building and training of surveillance tradecraft skills. These include specialisations in foot, mobile, aerial and technical surveillance methods.

Key Skills

- Qualified CIPD Training Instructor
- Discretion and Reliability from 25 years of experience in the field
- Highest level of Security Clearance in the United Kingdom including DV (Developed Vetting) and STRAP1 clearance.
- Planning Officer for the deployment of many high-profile surveillance operations
- Senior team-leader leading multiple surveillance teams on active operations against crime, political and terrorism related operations in conjunction with Specialist Police Units and UK Special Forces.
- Senior surveillance trainer responsible for the development and delivery of bespoke training packages for the MoD and partner agencies both from the UK and overseas.
- Specialist Foot and Vehicle Surveillance
- Specialist in Aerial Surveillance
- Specialist in Technical Surveillance (audio, photographic and tracking)
- Clear and Concise written communication skills to evidential standard
- Advanced driving skills

Career

1990 - 2014 Ministry of Defence

2013 – 2014 Surveillance Team Leader, leading my teams on proactive surveillance operations having responsibility for the effectiveness of the operation; while considering the pre-planned risk assessment against the ongoing dynamics. To manage any risk to personnel and operational security and to implement risk thresholds and exit strategies for any foreseen or likely adverse circumstances, communicating my plans clearly and concisely to the team.

2012 - 2013 Manager responsible for the governance and writing of Standard Operational Procedures relating to all aspects of surveillance operations and associated risk assessments
2010 - 2012 Management and development of the Service ”Operations Room” involving the dissemination of Intelligence and the proactive tasking of Service resources in a fast-changing environment due to multiple service operations being conducted simultaneously. During this period on the lead up to the 2012 Olympic Games I instigated a thorough restructure of the processes of this department.

2008 - 2010 Team-Leader for Service surveillance teams, this entailed leading operations and being the development and reporting officer for a team of surveillance operatives

2007 - 2008 Senior training instructor for both the Service and Specialist Police units having been tasked to ensure each service worked jointly to standardised procedures due to the proliferation of joint operations from the increasing threats to the United Kingdom.

2005 - 2007 Planning Officer responsible for strategic deployment of Service resources and Implementation of Service briefings both pre and post deployments to operational personnel and senior managers

2006 - 2007 Operations Rooms Manager, I introduced a full training package to standardise the working practices of this department which had a regular turnover of staff as this was considered a development posting for Service personnel seeking promotion.

2003 – 2006 Surveillance Team Leader responsible for the running of operations and leading a large team of Surveillance operatives on nationwide operations.

1999 – 2003 Seconded to “Service Academy” to deliver Agent Handling Skills and Surveillance Tradecraft to Service personnel, Special Forces and Special Branch. I was the SPOC for partner agencies from countries allied to the United Kingdom this would necessitate the creation of bespoke training packages for these agencies covering Surveillance, Counter Surveillance, Anti Surveillance and Agent Handling Activities. This required that I worked abroad including hostile environments as well as hosting these agencies as guests in London.

1997 – 1999 Promoted to Surveillance Team Leader responsible for running operations and leading a large team of surveillance operatives as their development and reporting Manager.

1990 – 1997 Induction and foundation training leading to my role as a Mobile Surveillance 0fficer. Tasked against Political targets of interest to HMG. Counter Espionage, Counter Terrorism and Serious related Criminal activities, Mentoring and Training of new operational staff.

Pertinent Qualifications/Courses

- CIPD Professional trainer for trainers Certified
- Presentational Skills
- Counter Hi-Jack and evasive driving trained
- Court Room Skills
- Advanced Driving trained
- Agent Handling Skills course
- Aerial Surveillance Trained (RAF)
- Covert Photography
- First Aid
- Navigational Skills Course
- Technical Beacon methods training

CV - Covert Operative 2B

Personal Statement

30 years of exemplary service with the Metropolitan Police Service. Highly skilled and experienced manager and operative in the world of security, fraud, covert intelligence, investigation, surveillance and risk assessment. Most of this experience has been gained in the field of counter terrorism drug trafficking and serious crime. I am fully surveillance and technical surveillance trained. I was also a fully trained Financial Investigator and have vast experience in Theft, Fraud, Money Laundering, Bribery and Commercial Corruption.

Employed in 2015-16 as a Security Operations Manager at Goldman Sachs Merchant Bank in London. I managed 275 security officers dedicated to the safeguarding of over six thousand employees on five sites across London.

Undertook a role as Head of Security at Barclaycard UK HQ. I had complete strategic control and overview of all matter’s security including budget. I had responsibility for staffing, training, site security and the terrorism policy which I rewrote on behalf of Barclays. In that time, I also reviewed all the existing financial contracts in place and changed the contracts and suppliers who were not providing contractual value for goods and services supplied. This saved Barclays vast amounts of money in the security budget.

Since April 2018 I have been a contracted by the Royal Mail on their largest ever Fraud case. The loss figure is around £90 Million, with £30 million in frozen assets and 11 subjects arrested who have now been charged with various Fraud offences. This Fraud spans the areas of Invoice and Procurement Fraud over Thirty different companies using Royal Mail services. During my employment I have been

additionally tasked by Royal Mail to handle Industry sensitive intelligence coming from the heads of national and international mail houses and I have been working within the Royal Mail Whistleblowing mechanism, where confidentiality and the handling of sensitive intelligence is of paramount importance to protect sources of intelligence.

Additionally, from my Police qualifications, whilst at Barclaycard I successfully completed a NEBOSH course around Health and Safety Management at work

Key Skills:

- Investigative and Cognitive Interviewing Course
- Surveillance and Technical Surveillance trained. Met Police and Home Office
- Advanced Driver. Police and Home Office trained.
- Field expert in the use and deployment of CCTV and both covert and overt camera's.
- Proficient in Microsoft office, excel, word and power point
- Police and Home Office Edexcel Financial Investigation Qualifications. (POCA)
- L3 City and Guilds Teaching Certificate.
- NEBOSH. Health and Safety management at work
- Excellent communication skills, both written, verbal and via power point.
- Excellent skills in risk assessment and risk awareness
- Strong interpersonal skills.
- Ability to work in high-risk security situations and manage crisis situations.
- Exceptional management skills having managed teams in both hostile and operationally demanding situations.
- Effective problem solving.
- Strong analytical and research skills.

Employment History:

- Metropolitan Police. Specialist Detective
- (1985 - 2015)

- Goldman Sachs. Security Operations Manager
- (Jan 2016 – June 2016)

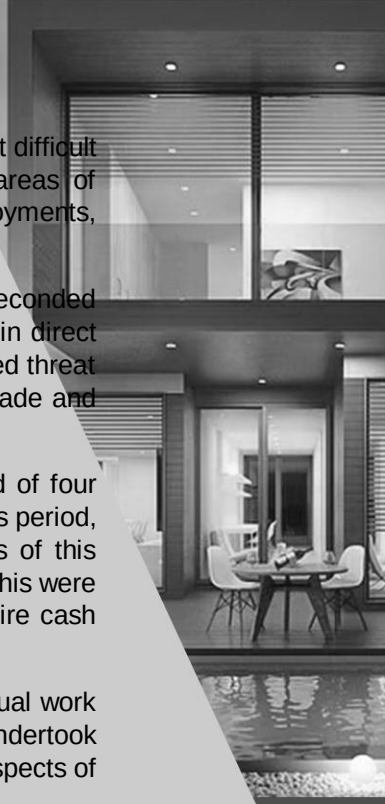
- Barclaycard UK HQ. Head of Physical Security
- (July 2016 – Nov 2017)

- Bastion-Solutions Limited 2015 – Current.

- Royal Mail Contracted Investigator April 2018

Summary of Police Experience

Experience



February 2013 to March 2015 - Technical Surveillance Unit. This is a covert post solving the most difficult surveillance issues in all aspects of serious and international crime. My work involved the areas of Terrorism, Murder, Kidnap, Contract Killing and Drug Importation. I was engaged in camera deployments, premises/vehicle technical attacks and covert communication data capture.

January 2012 to February 2013 - Metropolitan Police Counter Terrorism Command. This was a seconded post in the period leading up to and after the successful London Olympics. The project worked in direct partnership with the UK secret services to deal with intelligence and risk surrounding any UK based threat to the Olympic Games, with specific focus on terrorism and extremism. My role was to assess, grade and disseminate intelligence to proactive teams for operational purposes.

August 2009 to January 2012 - Metropolitan Police Cash Seizure Team. This team consisted of four Detectives engaged in seizing cash in proactive operations from London's top criminals. During this period, we seized approximately 3 million pounds of currency in both Euro and Sterling. The success of this initiative led to the financial ruin and disruption of many established criminal networks. My roles in this were as part of the surveillance team and I was the sole financial investigator responsible for the entire cash seizure process, from arrest through to court.

April 2005 to August 2009 - Metropolitan Police Economic Crime Unit. The focus of my individual work here concentrated on fraud, international money laundering and asset confiscation. On this unit I undertook all my relevant financial qualifications which remain current and in place. I am experienced in all aspects of using POCA. Proceeds of Crime Act reactively and proactively

April 2000 to April 2005 - National Crime Squad. (Now known as the NCA). On the National Crime Squad I was involved in the following successful projects. My individual roles on these projects were covert surveillance and investigation, including financial enquiries.

2000-2002 - Animal rights extremism project dealing with fanatical activists placing incendiary devices at the homes of employees involved in the pharmaceutical industry.

2002-2003 - Terrorism project located at Heathrow and Gatwick airport post the 911 bombings. This was in an effort to deal with internal staff corruption, which allowed people to bribe their way onto plans by bypassing normal security checks and searches, which in the light of how the 911 bombers were effective was rightly deemed a major terror risk.

2003-2005 - The Nottingham project - This was a covert operation ordered by the Government into the lawlessness in the City of Nottingham relating to gun and drug crimes within the city. My individual role here was as part of a covert surveillance team gathering intelligence and evidence.

Covert Operative 2C

See below Covert Operative 2D below very similar background now a qualified London Black Cab driver. Cannot access his CV as he is abroad and uncontactable until 25/01/2023.

CV - Covert Operative 2D

Proven track record of high-quality delivery in diverse, complex environments and roles over a 42 years of criminal and civil investigation. A natural leader of people with a strong commitment to professional development.

Expert knowledge and skills in law enforcement disciplines at numerous grades. I formerly served with HMCE/HMRC and the Serious Organised Crime Agency.
I have gained expertise in the private and public sector providing consultation and training services focused on a wide portfolio of investigation and intelligence skills including an emphasis on pre deployment due diligence.

Worked extensively on border issues (logistics and security), organised crime in the UK and overseas, including smuggling, counter narcotics, people trafficking, fraud, corruption and money laundering.

Managed teams of up to 100 people delivering organisational change whilst exploiting diverse procedures, cultures and attitudes. I build effective internal and external relationships, working collaboratively with stakeholders and external agencies in the UK and overseas.
Managed delegated budgets in excess of £1m whilst delivering efficiency savings and delivering on objectives.

KEY SKILLS

- Reliable and discreet: Highest level of security clearance in UK, DV (Developed Vetting). Currently UK government SC (Security Checked) clearance.
- 30 years Government Service, 12 years Private Sector
- 27 years Operational Organised Crime experience
- Former Head of Undercover Infiltration Unit, SOCA
- Former Head of Witness Protection and Assisting Offender Debriefing Unit, SOCA
- Former Head of HUMINT (Human intelligence), Compliance & Excellence and Training - Informant Handling, Undercover, Protected Persons, Offender Debriefing, OSINT & due diligence research team in SOCA.
- Former Head of Operational Security HUMINT (Human Intelligence), SOCA
- Former Head of Overseas Informant programme, HMRC
- Authorising Officer for Covert Human intelligence Sources & surveillance – HMRC
- Senior Investigation Officer – Head of Covert Human Intelligence Unit Southern Region and Intelligence extraction from intercept, HMRC
- Senior Investigation Officer – Head of Overseas Operational Intelligence Fraud Unit, South East Region Anti-Corruption Intelligence Unit, Intelligence Profiling Unit (using open source and closed source data), HMRC
- Undercover Unit – Management, Coordination and Operational duties including selection and training. Focus on maritime, money laundering, corruption and transport based organised crime.
- Highly experienced in investigations including Smuggling, Money Laundering, Corruption, Transport and Tax Frauds.
- Foot and vehicle surveillance operator and trainer in a specialist team

EMPLOYMENT HISTORY

2022/23 – Screening Interviewer for the Home Office Immigration Service. Employed by Global Secure Accreditation Ltd. Undertaking screening interviews of asylum seekers and illegal immigrants on behalf of the Home Office. Using interview and IT skills to interview persons seeking asylum, usually through interpreters, to ascertain the validity of their claim. Identification and referral of safeguarding issues, high risk and potential intelligence opportunities of refugees.

2021 – Liaison Officer – Managing and liaison between the Department of Health and Social Care**,** Hotel staff, medical and security staff for Global Secure Accreditation Ltd in government designated quarantine hotels to ensure the safety, security and welfare of persons held in quarantine during the COVID pandemic. Management of meetings and staff within the hotel overseeing and changing procedures where issues identified.

2010 – Present Director, Dextera Global Ltd. delivering a wide range of investigative services to clients. Providing expertise in a range of learning and development strategies in response to the increasing demand for training in response to transnational organised crime, terrorism and commercial threats including supply chain and physical and electronic penetration testing.
Undertaking commercial and overseas government training, investigations involving surveillance & intelligence gathering.
Open-source due diligence design (I-Trap system) and research. Leading the design, development and delivery of I-Trap system for operational and intelligence use focused on effective & focused due diligence.
Open source and dark web covert research investigator qualified.
Independent law enforcement adviser and trainer.

2019 – 2022 Fraud Investigator for BBFI and City of Westminster Council. Duties include investigating fraudulent activities within Westminster Council. Use of due diligence, surveillance, advanced interview techniques and enforcement action to prosecute offenders.

2005 – 2010 Grade 2 Serious Organised Crime Agency (SOCA)

- Head of Covert Infiltration Operations – the strategic and tactical lead of SOCA's undercover infiltration unit. Authorising and prioritising operations, developing of capability by innovative use of intelligence whilst ensuring legal and safety compliance of staff. Advising on legislation, policy and tactical options for effective deployments. Represented SOCA at national and international forums.
- Head of Witness Protection Operations – strategic and tactical responsibility for the risk assessment related to threats to witnesses and associated departmental persons. Undertook a comprehensive reorganisation of the department, setting the national standards for assessment and protection to ensure value for money and increasing security for protected persons. Introduction of due diligence to ensure the safety and/or abuse of the system by protected persons.

2002 – 2005 Senior Investigation Officer HMRC

- Authorising Officer and Head of Regional and International Informant Management Unit.
- Lead for Intercept Intelligence Exploitation Project.
- Use of witness protection techniques to combat organised crime.

2001 – 2002 Senior Investigation Officer HMRC

- Head of Anti-Corruption Intelligence
- Head of Overseas Anti-Fraud Organised Crime Disruption team
- Head of sea/road freight and passenger profiling intelligence team
- Head of intelligence gathering and profiling for intercontinental train freight traffic exploiting due diligence and closed data to identify offenders.

Covert Operative 3

Covert Open Source & Social Media Screening

DB – Internationally renowned leading expert on digital risk profiling and online investigations. DB works globally with many high-profile individuals across TV, film, music, sport and business. He provides bespoke personal service for his clients, and is also well known for his specialist work with law enforcement, defence and diplomatic sectors across the world.

Deliverable services:

Online exposure and risk assessment – Personal exposure of sensitive information. Information and detail accessed by criminal & political groups. In depth search of the internet for exposed data, including websites, social media, leaked and consented data. Risk profile of the client and analysis of level of vulnerability and mitigation.

Privacy and security strategies - digital privacy and security strategies to enable safe online and offline services and transactions, whilst minimising personal details. Assistance with subject access data and commercial intelligence. Minimise risk to personal data breaches. Minimise unwanted contact or intrusion via messaging apps, email & phone calls. Retention for ongoing support and advice.

Threat Investigation – Specialist online investigation and identification who may be behind the threats, and analysis of their backgrounds to assess threat level. Liaison with law enforcement and online companies to assist the threat as appropriate.

Data Removal - Advice to client regarding removal of information from online companies and government organisations to support removal from websites.

Background checks – In depth research of background and online presence of subjects as requested such as potential employees.

Communications Security Review and Protection Plan

- Laptop/phone/desktop security screening.
- Protection of electronic communication devices and offensive security advise where required.
- 2 laptops per day.
- Android devices simple and fast to screen for bugs, malware, phishing and virus's.
- iPhone are more difficult, take longer and need to have a different way to assess by planting software into the device which screens all traffic. The software can be removed if the client does not wish to have constant monitoring.
- A security review of all communication devices recommended.
- Security advice regarding hardening of the communication devices.
- Bespoke advice regarding secure behaviour when using communication devices and carriage.

Covert Operative 4

With more than 20 years working with Government, MoD, intelligence service and Policing both domestically and abroad helping and advising foreign governments in the matter of cyber from defensive, offensive and forensics.

This has given me a unique perspective on cyber warfare as I combine my knowledge of offensive (including state level attacking and cyber surveillance) with forensics, this knowledge has given me an insight into counter-cyber intelligence

After leaving the services I helped to build a one-of-a-kind cyber training agency that teaches a unique approach to cyber to both domestic and friendly government agencies.

Currently I look after the cyber of some of the biggest companies, high profile individuals and write and deliver bespoke training to domestic and friendly governments.

In regards to this situation I would highly recommend that each device undergo a forensic examination that will include the Operating system applications and communication channels cellular, Wi-Fi and Bluetooth.

Once examination is complete and any malicious code / exploit removed these devices should be hardened and a one to one with the client on best practice and their options in regards to keeping safe both online and the use of additional devices

DEPLOYMENT TASK: (COUNTER SURVEILLANCE-VEHICLE-FOOT)

Task Operation: **7-14-day Covert Counter Surveillance cover. (Vehicle-Foot)**

Planned and dynamic routes assessed with a view to identify hostile surveillance operatives. Experienced surveillance experts deployed to undertake the identification and video/photographic recording of suspected hostiles.

Operational Requirements:

- Use of trackers, normal routes with strategic stops, planned pattern for the day required in advance. Area sweeps carried out covertly.
- Tracker placements-Vehicle - person
- Client weekly schedule requirement
- Known routes taken daily (vehicle-foot
- Any key regular appointments-social-leisure programmes within each week period
    - Total lifestyle understanding on a weekly basis
        - Social calendar events
        - Gym membership and days of attendance
- Team premises needed nearby to respond quickly to any change in plans.
- TBC nearby monitoring building of clients premises

Post deployment:

- Report including recommendations and any follow up action
- Intelligence on any find
- Legal issues – We work to evidential standards in the UK

Cost Implications: are based upon first initial ground survey and findings evaluations for task requirements

- Initial survey & findings-recommended course of action plan
- Operational location: (Hotel or apartment)
- Daily rate for a team of x3-4 operative experts tbc
- All covert equipment hire; Radios-trackers- camera etc
- Vehicle hire and changed out every 2 days (x 2 vehicles x1 motorbike concept proposal).
- Admin and support requirements
- Applied VAT