



TSCM: A WHITE PAPER AND A RED FLAG FOR OUR CLIENTS AND FOR THE SECURITY INDUSTRY

By: Jack Nichols Mogus, Director-Special Operations, Nova Technical Services

"AN INFORMAL DISCUSSION"

WHAT ARE WE TALKING ABOUT HERE?

We, at Nova Technical Services, perform Technical Surveillance Countermeasures (TSCM) services. Sometimes it's called "Sweeping" or "De-Bugging" or sometimes "Electronic Countermeasures", sometimes "Eavesdropping Detection". It is a major component of the Information Protection Paradigm. It is *crucial* to the security, viability and prosperity of corporations, government entities and individuals. TSCM is a very complicated, arduous and demanding field of endeavor, and the state of the art is continually advancing, requiring frequent upgrading of equipment, procedures and training. Most people, even those in the Security Community, do not fully comprehend all that it entails when done properly. The movies and late night television don't begin to scratch the surface. The work is far more time consuming, technically complex and mentally and physically challenging. It is *also* very satisfying.

Nova has been in the security business for thirty-eight years. TSCM is the *only* thing we do. It's our life and our passion and we take it seriously - very seriously.

For several years now we – and others in the business – have been observing a disquieting trend. There have been a number of people attracted to the TSCM business who do *not* take it seriously. They are here because they think they can make a quick and easy buck. They have noticed that legitimate TSCM teams charge a respectable price for their services. They buy a few hundred or a few thousand dollars worth of gadgets and movie props and with no training and no experience advertise "Sweeping and De-Bugging" services. None of these guys perform TSCM services on a full time

basis. It's always a sideline to some other day job. When they get a "sweep job" it's usually a windfall to grab a few quick bucks on the side. They can certainly afford to underbid the legitimate companies who have hundreds of thousands of dollars invested in top of the line equipment, who have attended extensive training courses, who have years – or decades - of experience, who are legitimately in the business, who pay substantially for adequate business insurance, and who employ dedicated and highly trained technicians.

The purpose of this White Paper is to "call these guys out" – to shine a light on their operation so that clients may make informed choices when looking for a professional TSCM company. The more you know about the subject the better prepared you are to choose a TSCM provider who is going to make every possible effort to protect your valuable information rather than perform a quick Rain Dance and take your money and run.

TIME TO TAKE OFF THE GLOVES:

It is neither my style nor my intention to advance our professional business cause by "knocking" the legitimate competition. However, because of the horror stories we have all heard, because consumers deserve to know *all* the facts, because the information that we are trying to protect is *far* too important, and because there *are* people in the "Sweep Business" who should be jailed for fraud, I feel compelled to clear the air.

There are other legitimate TSCM practitioners out there besides Nova. Those who, like us, have dedicated themselves to the profession and who have invested large sums of money in top of the line technical equipment and long periods of time in training in order to provide proper TSCM services to government, business, industry and to individuals. These are our *real* competitors and we have *every* respect for them. Should you choose one of them over us you will not likely be hurt in the deal. However, there are charlatans, pretenders, wannabes and downright crooks out there; the guys with the \$800.00 or \$8000.00 "magic wands" who will offer to "sweep" your facility for a bargain basement price. Purchasing a few small pieces of equipment and placing an ad on line or in the Yellow Pages does not qualify a person to perform TSCM services.

Quite unfortunately, there is virtually no regulation of the TSCM business. People can make any claim they wish, profess any level of expertise, fabricate equipment inventory

lists, falsely claim previous life experience and, in general, invent any cock and bull story that they think will convince you to hire them. I've heard a lot of them. I've been embarrassed to hear some speakers at seminars and association meetings who make totally outrageous claims. It's all I can do to contain myself until I can speak to them afterward and challenge, in private, some of their preposterous statements. I have had some apologize – and thank me for not raising the issue while they were speaking – I have also had them shrug and say, “Hey, buyer beware”.

It is up to *you* to ask the serious questions: “How important *is* the information that I want to protect?” “How do I thoroughly *evaluate* each proposal and the people submitting it?” “Do these guys *really* have the right credentials and can they *prove* it?” “Is TSCM a *serious* business for them or is it only a – once in a while - sideline?”

A thorough TSCM inspection is not inexpensive. If someone's proposal sounds “too good to be true” you can be certain that it is.

The money that you invest in TSCM services can be the best bargain you will ever make – by protecting your valuable information – or, it could easily be the worst – leaving you with a false sense of security and because of this your information even more vulnerable than before. A professional TSCM service could easily save you *many* times the cost of that service. An incomplete or inadequate service could very well cost you hundreds of times more than the professional service would have been. Just one overlooked listening device or concealed camera can defeat the entire process. Consequently, money saved by using less equipment and inadequately trained personnel – the typical “cheap sweep” - can result in all of the money being wasted, leaving a false sense of security and thus actually increasing your risk of critical information loss.

You wouldn't consider letting someone who has taken a First Aid course perform open heart surgery on you – especially if he purchased his “surgical instruments” from Home Depot. That is *not* an unreasonable comparison between a legitimate, trained, experienced and properly equipped TSCM specialist and so many of the “pretenders” out there.

A CASE HISTORY: We recently submitted a proposal to a large company – a leader in their field. They wanted proposals from three different TSCM providers. One of the

other bidders was offering their “service” for less than half of our proposal. The client wisely discounted that offer in short order. The second company’s proposal was for about fifteen percent less than ours. After two “in person” meetings with the client and several phone calls and e-mails during which we did everything we could to accommodate their budgetary concerns without compromising their security, they decided to accept the lower bid. They liked us, they liked our proposal but, there was a difference of almost two thousand dollars. (It was a very large job.) I thanked them for their time and for the opportunity to submit a proposal for the work. I informed them that I was sorry but I could not lower my price. We had priced the job at the lower end of profitability and I just could not reduce it further. What I did *not* say – and, in retrospect, *should* have said - was that there was no way that the other company could possibly do the same TSCM job that we proposed for the amount of money in their bid.

Our proposal included four technicians working twelve to fourteen hours on Saturday and on Sunday and eight hours on Monday. We also bring nine large cases of equipment to the job site. This amount of equipment is not unusual for a properly equipped TSCM team.

We were informed three weeks later – by a very frustrated security director - that the company that underbid us by fifteen percent had been scheduled to begin work at 7:00 AM on Saturday but did not arrive until 11:15 AM. Two men showed up – each carrying one briefcase - and they “finished work” and left the facility at 6:45 PM that same evening – a total of seven and a half hours. That was it!

The Security Director, who was our contact, was *deeply* concerned. The company, evidently, had just thrown a lot of money down the plumbing. He had two choices: He could go back to management and explain that they had made a *serious* and *expensive* mistake and recommend that they take his word for it and spend even more money to have the work done correctly or, he could remain silent – leaving his company at serious risk – and hope for the best. In as much as it was a very expensive mistake he felt that the repercussions could very likely make it a career limiting event for him. In any case he would have serious problems explaining it all to his superiors.

He chose to keep it covered up. I felt terrible for him. I felt terrible for his company. I was furious with the charlatans that had literally stolen from them. Litigating against the “TSCM Company” was not an option for him. They had a signed contract which only stated that a TSCM service would be performed – without any real specificity as to what

would be done. He had *assumed* that they were going to provide the same services that we had described in detail for him in our proposal.

His company was “screwed”. We’ve all heard the expression, “You get what you pay for”. However, in this instance as well as many other similar cases, the company got nowhere *near* what they paid for.

How could they tell? How could they have known?

Many of the “pretenders” realize that if they price their services for what they are *really* worth their deficiencies will immediately become obvious. Their solution? “Jack-up the price” to something *close* to what a real TSCM team would charge. Underbid by a thousand or two and hope that nobody asks the tough questions.

This incident is, in large measure, the driving force behind this paper. I have seen/heard this story repeated – with some variation – many times over the past three decades. This time it just disturbed me more than usual. Our contact, the Security Director, is a good man. He’s honest and a very loyal employee. He was placed, through no deliberate fault of his own, in the position of having to choose between telling his employer the truth and compromising his career – of over twenty years with his company – and remaining silent and compromising his company’s security. Not a nice choice. I sincerely regret not “taking the gloves off” when he informed me of the choice to hire the “other guys”. I saw it coming. I suspected what was going to happen. I had seen it too many times before. I just didn’t realize exactly how outrageous it would be. I chose not to tell him the facts, as I saw them, because I didn’t want to appear “pushy” or self serving - and out of some misguided sense of professional courtesy to the *competition* - to people who were not, in the least, professional. Yes – I’m angry with myself as well, and I will *not* make that mistake again. Sure – I was disappointed in not getting the job, but I’m furious about the fraud that was perpetrated against a good company and a good man.

WHO – EXACTLY – ARE YOU DEALING WITH? Are they really even in business or are they just “moonlighting” in order to pick-up a few extra bucks on the side? If they are in business – exactly *what* business are they in?

“Tom” was a guy in Fairfax, Virginia who owned a small plumbing business. Tom may very well have been a good plumber. Tom had a hobby – or rather a fixation – with all things clandestine. He was a great Robert Redford fan. He subscribed to several “Spook” magazines that are published mostly for the entertainment of pretenders and wannabes. After reading some of the ads in the back of a magazine he decided to order some “Sweep Gear”. He scraped together about \$800.00 and purchased several little plastic boxes. (Side bar here: \$800.00 would not quite cover the cost of only two of our larger equipment cases – without the equipment.) Tom’s new little boxes each contained a switch or two; one of them even had a little red light, another had a small meter. He had some fun “sweeping” his friends houses. Then he decided that with his new sweep equipment and his vast experience he should now enter the Sweep Business. Tom was shrewd. (He *had* watched a lot of TV.) He called me and asked me to give him an estimate to Sweep his plumbing shop and office. He used the pretense that he believed his wife was “spying” on him. He was very interested in just how we priced our services. Of course, he never contracted for our service. This really did not surprise me. Tom’s whole story just didn’t pass the “smell test”. However, about two weeks later one of my technicians showed me an ad in a small local newspaper “business card” section. The ad was for “Sweeping and De-Bugging Service”. The ad contained Tom’s name and the phone number of his plumbing shop. Our technician said, “Isn’t this the guy - - - - ?” I told her, “Yep, that’s our Tom.” For the fun of it, she called Tom and asked him to give her a proposal to Sweep her apartment. He came to her apartment, dressed rather well as it happened, and gave her an estimate exactly one half of what I had offered him to do his plumbing shop and office. He even showed her his briefcase full of equipment (all three pieces). His credibility fell even further, however, when he tried to convince her that the equipment had cost “several thousands of dollars” and that it was the very same equipment being used by the CIA. (Actually, she said it did bear a significant resemblance to the stuff used by Robert Redford in a recent late night movie.) Some months later Tom graduated to a small ad in the Northern Virginia yellow pages – still using the same phone number as his plumbing business – only now he answered the phone simply with “hello”; non-committal until you told him whether you wanted your office swept or your toilet flushed. I’m sure the term Caveat Emptor rings a bell.

Don’t be fooled either by the guys who claim expertise in TSCM because they, allegedly, were previously in Law Enforcement, or Secret Service, or CIA, or FBI, or *Whatever*. Perhaps they really were employed by that agency at some point; that does not support

a contention that they have *any* experience in TSCM. I mention this because I have met several people who make that assertion (and they even do it with a straight face).

May I suggest that you *demand* to see the business licenses, training certificates and other credentials of anyone with whom you consider doing business? Trust me on this one: Anybody legitimately in the TSCM business will be absolutely delighted to produce their credentials.

LET'S TALK ABOUT INSURANCE:

What happens if you hire an uninsured or under insured TSCM person? Let's say that the guy you hire gets his buddy to help him on the job (this happens every day – it's highly typical with small operators). His buddy slips and falls from the ladder while inspecting the overhead of the ceiling. His buddy is seriously injured. He files a Workers Compensation claim against his friend who hired him. But – his friend doesn't have Workers Compensation insurance. Guess who is going to get sued for the "employee's" medical expenses and lost time and lost income from his *day job*? Well, of course, he's going to sue the guy who hired him. What if the guy who hired him – the guy who couldn't afford to purchase Workers Compensation insurance can't, or won't, pay all of his friend's medical expenses and for his lost income? Guess who his attorneys are coming after next? Do you have a mirror handy? Ever heard the expression "deep pockets"? (Ask any lawyer.)

In most jurisdictions Workers Compensation Laws declare that an injured employee's "Exclusive Remedy" (a legal term) is through a claim against his employer's Workers Compensation Policy. This works just fine – provided that his employer *has* Workers Compensation insurance. If no such policy exists – all bets are off. The only thing you can count on is that *somebody* is going to be sued. Sometimes this requires some *Creative Litigation*, but that's what lawyers do. As one Personal Injury Attorney informed me, "I can firmly say that, in this instance, the client's exposure to litigation is 100%. They **will** be sued simply because they **can** be sued". You can be quite certain that if somebody is injured, and there is no insurance coverage for it – somebody is going to get sued. People are injured on the job every day. Sometimes very seriously. (Read *seriously* as *expensively* here.) Perhaps fatally. (*Really* expensively.)

Beyond the cost of medical expenses and compensation for his lost time from his *day job* is the problem of adverse publicity. What happened, who it happened to, where it happened and who was sued as a result all becomes a matter of public record. What Workers Compensation insurance does is insulate the *legitimate* employer from the devastatingly high costs of medical and lost time and income expenses. When the employer is thus insulated – so are you.

That's just Workers Compensation. How about all of the other tragedies that should be insured against? What would happen – and who would be held financially accountable – if your TSCM contractor accidentally “blew out” a large part of your telephone PBX system severing your communications to the outside world for a day or two or even longer? What if his actions accidentally caused a fire? How about if he inadvertently caused an electrical short circuit – tripping a circuit breaker controlling critical electrical equipment? What happens if his careless use of tools (as is in left lying about) causes injury to one of your employees or to a visitor to your company? Don't take anyone's word for their having proper insurance. “*He told me he was insured*” is not an adequate defense – in court or in front of your boss. Demand to be shown insurance certificates. Better still – require that you be listed as an “Additional Insured” on a separate Certificate endorsed by his insurance carrier and given to you for your records. Your TSCM Company can have this faxed or e-mailed to you in a matter of minutes. Don't let them begin work without it. Don't take that risk.

Sure – you might save a few hundred dollars by hiring the *cheapest* company. However, will it be worth that *few hundred dollars* when you are slapped with a law suit for a *few million dollars* because of a personal injury or you are faced with many thousands of dollars in property damages to your facility? It's Not about Lowest Price that matters – it's about Best Value.

It takes only **seconds** for something really bad to happen causing a serious personal injury or major damage to your infrastructure. It can take **years**, many **dollars** and much **aggravation** to resolve the matter.

At Nova, ALL of our technicians are “W-2 Employees”. No sub-contractors. No borrowing the brother-in-law for the weekend. Our employees are covered. We are covered. YOU are covered.

Make certain that you are protected from the person who is going to protect your valuable information.

We live in a very litigious society. Please take the time to insure that you are protected from embarrassing and expensive legal actions as well as from damage to your facility.

Any person who is smart enough to be a legitimate TSCM practitioner is certainly smart enough to understand these risks and to properly insure against them. He or she will also be very happy to show you all of their credentials.

The cost of *not* protecting your vital information could be very significant. The cost of doing the job incorrectly or inadequately could be *devastating*. Few things could be worse than having a false sense of security – believing your information is secure when, in fact, it's not.

REAL vs. REALLY?

A question you might hear from *amateur* TSCM folks is, “Why would you hire that *expensive* TSCM Company? Do you really think you need protection from the CIA or the Russians?” If they ask those questions – or some variation thereof - simply don't waste your valuable time with them. They are, in fact, admitting that they do not have the equipment, training or experience to be doing proper TSCM work. Much of the Spy Gear available to serious hobbyists, private investigators and just about anyone with a desire to acquire it is nearly indistinguishable from some of the surveillance equipment used by many governments. Identifying and locating even cheap amateur Spy Gear still requires much of the same level of technical expertise and equipment as employed in securing a government installation. The pretenders are just not going to be able to do the job with a box full of spy shop gadgets and movie props. In the end – it all comes down to Experience, Equipment and Training. Remove any one of the three from the equation and you have a condition that will all but certainly result in failure. Failure – in the TSCM business - is simply not acceptable. The failure to receive adequate service for your money is a minor concern. The failure to protect your valuable information could have tragic results. Going back to that same person with First Aid training and the “surgical instruments” purchased from Home Depot - would you let him perform brain surgery on you because – after all – it's only a *small* tumor?

LET'S FACE IT:

When you're shopping for TSCM services and you look on line or at a yellow page ad or a business card, Tom, the plumber, and I look pretty much the same. (He may be better looking but I like to think I appear more distinguished.)

The difference becomes very apparent, however, when you compare credentials.

You should *demand* to see copies of the following items – at a minimum:

- Business License – showing the type of business.
- Insurance Certificates - Especially for Workers Compensation, Professional Liability (Errors and Omissions) and Completed Operations. A minimum of one million dollars. (Our coverage is for three million dollars.)
- Training Certificates for TSCM courses - at least four or five but – the more the merrier. (I carry copies of twelve of them in my brief case.)
- Professional Association memberships – again – four or five at least – *and* – they should all be related to Information Security, Communications, Intelligence, Etc. (We belong to ten such organizations.)
- An Equipment Inventory listing at least the major pieces and their manufacturer.
- Photographs of the major pieces of equipment; Real Photos of *his* equipment, not a manufacture's brochure.
- A Complete – and detailed Proposal, showing what tests/inspections will be conducted, what equipment will be used, the ranges/capabilities of the equipment, the estimated man hours and the number of technicians that will be used.

Many people who advertise “sweeping” and “de-bugging” services make their living spying on spouses and watching insurance claimants in hope that they will work out at the gym today – and – “oh by the way – we can sweep your home or office for you with our brand new \$800.00 Sweep Kit with which we have had absolutely no training”.

We have many good friends who are Private Investigators. They are competent, honest and professional people. We work *with* and *for* many of them. If we need an investigation conducted – we call them. If they need TSCM work – they call us. We also sub-contract as a Technical Support Team for several of the finest Investigative and Security Services in the country.

A TSCM service provider is asking you to take a lot on faith. You're going to give them a lot of money to perform a service with which you have – at best – a passing familiarity. (If you were an expert you wouldn't call them to begin with – you'd do the work yourself.) They should be happy to brag about their credentials. We certainly are. As President Ronald Reagan said: "Trust – but verify".

Nova Technical Services, a division of Avalon Corporation, has been in business since 1971.

Nova is a Veteran Owned Small Business, certified to perform TSCM Services for the U.S. Government.

© Copyright 2010, Avalon Corporation. All rights reserved.