



PO Box 316, North Chili, NY 14514 • (585) 889-2321 (voice) • (585) 889-0823 (fax)  
www.cisginc.com • info@cisginc.com

---

## **Technical Surveillance Counter-Measures Class Reservation Form**

Counter Intelligence Solutions Group, Inc., welcomes your interest in our TSCM class. This class is accredited by the State of North Carolina Private Protective Services Board as part of our Counter Intelligence School. Please fill out this form to reserve your seat in our next class scheduled for **February 3<sup>rd</sup> to 7<sup>th</sup> 2003**. Our location for this class is yet to be determined, however it will be in the greater Tampa, Florida area. We will supply you with a list of hotel names / phone numbers, and our special room rates as it becomes available in the next coming months. Scheduling your flight for Tampa International Airport (TPA) is recommended as the hotel will be within 10 minutes for that airport. The course is scheduled for 48 hours of training – our curriculum is attached for your reading enjoyment. This is *hands on training*, not simply classroom instruction. The price per student is \$1495.

Please fill out this reservation form completely, and return it as soon as possible to ensure your seat will be reserved. Seating is limited to 15 individual attendees per class.

Name of Student(s): \_\_\_\_\_

Company Name: \_\_\_\_\_

Address: \_\_\_\_\_

City/State/Zip/Country: \_\_\_\_\_

E-Mail Address: \_\_\_\_\_ Phone Number: \_\_\_\_\_

If Private Investigator, List State & License #: \_\_\_\_\_

Do you or your company currently offer TSCM/Sweeps now? ( yes / no )

List any sweep equipment you currently use: \_\_\_\_\_

List any areas of interest not covered by curriculum: \_\_\_\_\_

Please return this reservation form, and include a 50% non-refundable deposit per student, or the entire \$1495 amount per student. There is no sales tax unless you are a New York State resident. Full payment for the class is required prior to January 1<sup>st</sup> 2003. Reservations are guaranteed upon receipt of deposit. Please mail this form to: CISG Inc., PO Box 316, N. Chili NY 14514.



# **Technical Surveillance Counter-Measures**

## **Course I Curriculum**

- Contact Hours:** 48 hours of classroom and practical hands on training
- Prerequisites:** None
- Comments:** A basic understanding of electronic theory and/or radio theory is helpful, but not necessary.

Counter Intelligence Solutions Group, Inc.  
PO BOX 316  
N. Chili, NY 14514  
585-889-2321

## **Day One – Morning – 4 Hours**

- I. Introduction to TSCM**
  - A. Introductions**
  - B. Course Overview**
    - 1. Capabilities after taking course**
    - 2. Continued education/training**
    - 3. Classroom and hands-on training**
  - C. Technical Surveillance Counter-Measures II course overview**
  - D. Technical Surveillance Counter-Measures III course overview**
  - E. Why do we need TSCM?**
  - F. Terms and definitions**
  - G. Laws concerning electronic surveillance**
    - 1. Omnibus Crime Control and Safe Streets Act of 1968**
    - 2. Economic Espionage Act of 1996 (EEA 96)**
    - 3. State and Territorial Consent laws, one and two party consent laws**
  - H. Warning signs of possible eavesdropping**

## **Day One – Afternoon – 4 Hours**

- II. Basic Electronics**
  - A. Basic theory of transmitters and receivers**
    - 1. Component identification**
    - 2. Types of modulations**
      - a) FM**
      - b) AM**
      - c) Phase**
    - 3. Antenna theory**
    - 4. Power theory**
    - 5. Radio frequency spectrum**
    - 6. Frequencies used**

## **Day Two – Morning – 4 Hours**

- I. What type of threat exists?**
  - A. Threat Level I – Low level threat (Define / Examples)**
  - B. Threat Level II – Intermediate level threat (Define / Examples)**
  - C. Threat Level III – High level threat (Define / Examples)**
  
- II. Types of bugs, taps and other eavesdropping devices**
  - A. Basic overview of eavesdropping devices (critical components and makeup)**
  - B. Types of devices (low level threat)**
    - 1. Radio Frequency Transmitters (RF)**
    - 2. Hardwired devices**
    - 3. Contact microphones**
    - 4. Inductive devices**
    - 5. Burst transmitters**
    - 6. Frequency hopping devices**
    - 7. Microwave transmitters**
    - 8. Infrared devices**
    - 9. REMOBS**
    - 10. Series Taps**
    - 11. Parallel Taps**
    - 12. Infinity Transmitters**
    - 13. Laser listening devices**
    - 14. Light modulating devices**
    - 15. TEMPEST**
    - 16. Video devices**
    - 17. Carrier current devices**
    - 18. Drop-out relays**
    - 19. Hookswitch bypass devices**
    - 20. Body wires**
    - 21. Bumper beepers**
    - 22. Other devices**
  - C. Other threats**
    - 1. Intercoms**
    - 2. Wireless microphones**
    - 3. Baby monitors**
    - 4. Hot mic telephones**
    - 5. Public address systems**
    - 6. Extension phones**
    - 7. Bridging a tap**
    - 8. Tape recorders**
    - 9. Other devices**

## **Day Two – Afternoon – 4 Hours**

- III. Elements of a TSCM Sweep**
  - A. Client Interview**
    - 1. Qualifying the client**
    - 2. Identifying the threat level**
      - a. Who do you suspect?**
      - b. What are their resources and capabilities?**
      - c. Areas to be swept / searched?**
      - d. What to do if an eavesdropping device is found?**
      - e. What to do if a law enforcement device is found?**
    - 3. Client confidentiality**
  - B. Written proposal**
    - 1. Scope of sweep**
    - 2. Physical parameters of sweep / search**
    - 3. Technical parameters of sweep / search**
  - C. Acceptance and scheduling of a TSCM engagement**
  - D. Sweep Plan**
    - 1. Sweep team members**
      - a. Sweep team leader**
      - b. Telephone technician**
      - c. Physical security technician**
      - d. Electronics technician**
    - 2. Pre-sweep briefing**
      - a. Benefits of a written checklist**
    - 3. Post-sweep conference**
  - E. The Sweep**
    - 1. Non-alerting electronic search**
    - 2. Non-alerting telephone sweep**
    - 3. Alerting telephone sweep**
    - 4. Alerting physical search**
  - F. Internal report / notes**
  - G. Clients verbal report**
  - H. Clients written report**

## **Day Three – Morning & Afternoon – 8 Hours**

- IV. Non-alerting Electronic Search**
  - A. Types of equipment used to conduct an electronic search – capabilities and limitations of each**
    - 1. Spectrum analyzers**
    - 2. Oscilloscopes**
    - 3. Wide-band monitors**
    - 4. SWS meter**
    - 5. Scanners**
    - 6. Receivers**
    - 7. Frequency Counters**
    - 8. VLF receivers**
    - 9. Tape recorder detectors**
    - 10. Video camera detectors**
    - 11. Other equipment**
  - B. Equipment trade-offs: reliability, weight, capabilities, price, performance**
  - C. Hands on training**
  - D. Baseline reading and record keeping**

## **Day Four – Morning & Afternoon – 8 Hours**

- V. Telephone System Overview**
  - A. Basic telephone theory**
  - B. Types of telephone systems**
    - 1. Electromechanical**
    - 2. Electronic**
    - 3. Digital**
  - C. Telecommunication Devices**
    - 1. Hardwired telephones**
    - 2. Cordless telephones**
    - 3. Fax machines**
    - 4. Telex machines**
    - 5. Answering machines**
    - 6. Modems**
    - 7. Cellular telephones (analog, digital & satellite)**
    - 8. PBX/KSU units**
    - 9. Voice mail systems**
  - D. Other Telephone Equipment**
    - 1. Telephone lines**
    - 2. Distribution Closets / Frame Rooms**
    - 3. Central Office**
    - 4. Drop Lines / Appearances**
    - 5. Fiber Optics**
    - 6. Other Equipment**
  - E. Hands on training**
  
- VI. Non-alerting Telephone Search**
  - A. RF sweep of phone lines (on and off hook)**
  - B. Visual Inspection**
  - C. Hands on training**

## **Day Five – Morning & Afternoon – 8 Hours**

### **VII. Alerting Telephone Sweep**

#### **A. Telephone instrument and related equipment testing**

- 1. Wet line time domain reflectometer (TDR) testing**
- 2. Dry line TDR testing**
- 3. Line balancing**
- 4. Resistance Testing**
- 5. Physical inspection of telephone instruments and related equipment**
- 6. Digital voltage meter (DVM) tests**
- 7. Telephone line analyzers / testers**
- 8. Lineman's handset**
- 9. Tone generators**
- 10. Other tests**

#### **B. Hands on training**

### **VIII. Alerting physical search**

#### **A. What should be searched?**

#### **B. How to conduct a physical search (search patterns)**

#### **C. Practical tips and techniques**

#### **D. Equipment needed to conduct a physical search**

- 1. Non-linear junction detector (NLJD)**
- 2. Basic tools**
- 3. Electronic stethoscope**
- 4. Other equipment**

#### **E. Hands on training**

## **Day Six – Morning – 4 Hours**

- IX. Business Considerations**
  - A. Business aspects of TSCM**
    - 1. Record keeping requirements
  - B. Licensing requirements**
  - C. Insurance**
    - 1. Liability
    - 2. E&O Coverage
  - D. Aspects of working outside the United States**
  - E. Transportation of equipment outside of the United States**
  
- X. Preventative Measures / Proactive Approach to Information Security**
  - A. Cordless and cellular telephone vulnerabilities**
  - B. Voice / Computer encryptions**
  - C. Scramblers**
  - D. In-room monitoring**
  - E. Acoustic noise generators (ultrasonic sound)**
  - F. Random follow-up searches**
  - G. Access control**
  - H. Telecom security**

## **Day Six – Afternoon – 4 Hours**

- XI. Review Session**
- XII. Question and Answer Period**
- XIII. Additional Hands On Training**
- XIV. Closing Remarks**