



DEPARTMENT OF THE NAVY

OFFICE OF THE SECRETARY

1000 NAVY PENTAGON

WASHINGTON, D. C. 20350-1000

SECNAVINST 3850.4

N09N2

08 DECEMBER 2000

SECNAV INSTRUCTION 3850.4

From: Secretary of the Navy
To: All Ships and Stations

Subj: TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) PROGRAM

Ref: (a) DOD Instruction 5240.5 of 23 May 84 (NOTAL)
(b) OPNAVINST 5530.14C of 10 Dec 98 (NOTAL)
(c) DCID 1/21 of 29 Jul 94
(d) TSG Guides
(e) DCI Procedural Guides 1, 2, and 3 (NOTAL)

Encl: (1) TSCM Support Requests
(2) Technical Support Units

1. Purpose. To implement the policies set forth in references (a) and (b), update policies, responsibilities, and procedures for the Department of the Navy (DON) Technical Surveillance Countermeasures (TSCM) program, and to renumber the instruction per current standard subject identification codes.

2. Cancellation. SECNAVINST 5500.31A.

3. Definition. TSCM Survey. A comprehensive physical and electronic examination, by qualified personnel, of a facility's infrastructure, computer systems, office equipment, and communication systems to detect the presence of technical surveillance devices and hazards, and to identify technical security weaknesses that could aid in the conduct of a technical penetration of a facility.

4. Background. Historically, foreign intelligence services (FIS) have employed technical surveillance devices in espionage operations directed against U.S. installations, both in the United States and abroad. The devices employed have fallen generally into three groups: wired microphones, modified telephone and inter-communication systems, and radio frequency (RF) transmitters; however, other methods have been used. Technology suited to clandestine surveillance applications, which is available now to virtually everyone, has increased the risk of technical surveillance penetrations. Technical surveillance countermeasures, applied effectively, can limit both the ease with which surveillance devices can be employed and their ultimate success. References (b) and (c) address physical

08 DEC 2000

security measures to be considered when establishing positive access controls for sensitive discussion areas. Reference (d) addresses the special considerations for telecommunications and related equipment within secure discussion areas. Local security measures, implemented under the above guidance, can be augmented with TSCM support to detect the presence of technical surveillance devices.

5. Policy

a. Protecting sensitive discussion areas from technical penetration is the responsibility of every Commander. A comprehensive security program shall be established for the protection of all sensitive discussion areas. When discussions at the SECRET level or above are held within a space on a daily or otherwise regular basis, this security program shall include TSCM support performed by qualified TSCM personnel. Per the guidelines of reference (a), the Naval Criminal Investigative Service (NCIS) is designated to manage the TSCM program for the Department of the Navy (DON). The Director, NCIS shall designate a TSCM Program Manager to coordinate and implement the DON TSCM program. The NCIS TSCM Program Manager is responsible for providing TSCM support, technical direction, and centralized management of all DON TSCM assets and their utilization. Additionally, the NCIS is the sole activity within DON authorized to procure and use equipment for TSCM purposes, except for designated U.S. Marine Corps (USMC) Counterintelligence (CI) Teams. These Marine Corps CI teams shall procure approved equipment through the Marine Corps Supply System. When not deployed in combat support of the Marine Corps, Marine Corps CI teams shall also provide TSCM support as requested by the TSCM Program Manager. The support of the Marine Corps CI teams shall be primarily for Marine Forces (MARFOR) commands and secondarily for the support of other DON and Department of Defense (DOD) commands. To protect sensitive operations, all requests for support and correspondence shall be directly conveyed between the NCIS TSCM Program Manager and the appropriate Marine Corps CI Team Commander.

b. Navy and Marine Corps activities shall submit requests for TSCM support to the NCIS TSCM Program Manager. This restriction includes support for sensitive DON-sponsored projects at contractor facilities. Requests for TSCM services shall be accepted only for those facilities or categories of facilities that the NCIS TSCM Program Manager has determined to be probable and feasible targets for technical espionage.

c. A Tri-Service Memorandum of Understanding exists between the Director, NCIS and counterpart agencies of the Army and Air Force to provide for cross-service TSCM support in certain overseas locations. Although these assets may support DON activities, the responsibility for approving, requesting, and coordinating such support remains with the NCIS TSCM Program Manager.

d. TSCM surveys will be conducted per references (a), (e), and this instruction. TSCM personnel shall also evaluate the applicable spaces for technical and physical security vulnerabilities and, when necessary, provide recommendations to eliminate any security deficiencies identified.

6. Procedures

a. Selection of Spaces Requiring TSCM Support. Due to the cost of technical manpower, travel, and equipment, selectivity shall be exercised in identifying spaces to receive TSCM support. Support will be provided based on sensitivity, vulnerability, and risk management principles. Requests for surveys of facilities that are not used normally to discuss classified information and that are open to uncontrolled access by uncleared personnel shall be approved only if no other suitable facility is available. Surveys of such facilities have proven counterproductive by giving the occupant or occupants a false sense of security and by using limited TSCM assets that could be used more productively in other, more sensitive facilities. The following additional guidance applies:

(1) Qualifying Spaces/Facilities. Predicated on manpower and equipment availability, support will be provided to Special Access Programs (SAP) and Sensitive Compartmented Information Facilities (SCIF) in compliance with reference (c). This support can also be provided to those spaces where discussions classified SECRET or above routinely take place and have continuous access controls established as part of an effective security program to preclude undetected access. Guidance to achieve this objective is contained in references (b) and (c).

(2) Conferences. Conferences, symposia, exhibits, clinics, conventions, and meetings involving classified discussions shall be held in spaces, commensurate with the sensitivity of the information being discussed, that either have received or would otherwise qualify for TSCM support as set forth in paragraph 5a(1). When such facilities are not available and the information scheduled for discussion is classified TOP SECRET, one-time meetings may be supported if they are held in

08 DEC 2000

facilities not open to the general public, have the potential for good audio and physical security, have access control to the facility established prior to the TSCM survey and continued thereafter and throughout the conference.

(3) Flag Offices/Residences. TSCM surveys of flag offices and permanent quarters, because of their target ability, may be provided despite minimal security provisions, if doing so will not impact the completion of primary facility surveys. Priority consideration will be given to locations outside the United States where the FIS threat is greatest. It should be noted that TSCM surveys conducted under such conditions have no residual value and it cannot be assumed that after the survey such spaces will continue to be safe for sensitive discussions.

(4) New/Renovated Facilities. New installations or spaces having undergone major renovations will not receive TSCM support until all construction is completed, the spaces are manned, fully operational, and security measures are implemented. Direct pre-construction liaison with the nearest TSCM Support Unit is encouraged to ensure the standards set forth in references (b) through (d) are understood clearly and incorporated into the construction or modification plans. A request for pre-construction support does not constitute a request for TSCM support, and a written request for support, as set forth in enclosure (1), must be made once the facility is completed. Technical support units are listed in enclosure (2).

(5) Automobiles. TSCM support for automobiles will not be conducted unless justified by extraordinary circumstances. Such support can only be of value when the vehicle is kept under continuous physical security and maintained by cleared personnel.

(6) Ships and Aircraft. TSCM support will not be furnished to naval ships or aircraft unless justified by extraordinary circumstances.

(7) Data Processing Facilities. In addition to the foregoing criteria, areas that routinely process classified material utilizing computerized systems may justify TSCM support. TSCM personnel may investigate computers, networks and telecommunications systems to identify technical compromise or the exploitation of digital data processed or stored on these systems. Protective measures can be recommended to enhance the protection of digital information from threats of hacking computer or telephone networks and foreign intelligence exploitation.

00 DEC 2000

(8) Optional Facilities. In the interest of protecting sensitive/classified information, facilities may be selected by NCIS TSCM Program Manager for a TSCM survey. In such cases, the selected facility will be notified prior to the survey in order to coordinate the required command cooperation to complete the survey.

b. Recurring TSCM Support. No facility will qualify automatically for recurring TSCM service. In principle, once an area has been the subject of a fully instrumented TSCM survey with favorable outcome, the results are considered valid as long as the security integrity of the facility is maintained. Additional support may be requested when:

(1) There is documented evidence to suggest an area has been technically penetrated.

(2) Extensive construction, renovation or structural modifications have required unescorted access by uncleared individuals.

(3) Unauthorized personnel have gained uncontrolled or unescorted access to the secure area. In the interest of both good security and economy of resources, it is incumbent on commands to maintain the security integrity of sensitive facilities and to keep the use of this contingency to a minimum. TSCM surveys alone cannot substitute for good physical security and access controls.

c. Operational Security (OPSEC). TSCM services are highly specialized counterintelligence investigations, and as such, are particularly vulnerable to compromise. All commands that provide or receive TSCM services are required to implement OPSEC measures to ensure the success of the countermeasures effort. For this purpose, it must be assumed until the survey indicates otherwise, that a technical penetration has occurred. Should discussions concerning the pending TSCM support take place within the space, the device would likely be removed prior to the survey and later reinstalled or simply be switched off remotely. Under such circumstances the probability of surfacing a clandestine intercept device is greatly diminished. For this reason, discussion or verbal comments concerning the pending TSCM support shall not be permitted in the spaces of concern. Written requests for TSCM service are to be handled at the SECRET level and the number of persons apprised shall be kept to an absolute minimum. Telephone requests for TSCM support are considered compromising and are discouraged.

7. Action

a. Requests for TSCM support to augment a comprehensive security plan should be submitted by 1 November for the next calendar year (CY) scheduling. Due to manpower constraints, all routine requests for TSCM service may not be fulfilled and will be handled on a prioritized, first-come, first-serve basis each calendar year. A request for TSCM support shall be valid for a period of two years. Unanticipated requirements shall be submitted at least 60 days prior to the requested visit, and extenuating circumstances that require a faster response shall be clearly identified and fully justified within the request. Requests shall be submitted as stated in paragraph 5 and enclosure (1).

b. Due to the sensitive nature of TSCM support, correspondence that identifies upcoming visits and dates shall be kept to an absolute minimum. Requests for TSCM support shall be acknowledged upon receipt and scheduled for completion during the upcoming calendar year, if possible. Notification of TSCM support will be provided no more than 30 calendar days prior to arrival of the survey team. Normally, no additional correspondence will be initiated to reduce opportunities for compromise. If there is a change in a facility's status, point of contact (POC), or unforeseen circumstances arise within the requesting command which would preclude a visit, the NCIS TSCM Program Manager shall be notified immediately. Failure to do so may result in the cancellation of the scheduled survey.

c. Commands shall ensure that weaknesses identified as a result of TSCM services are corrected. Unless otherwise justified, TSCM support shall not be provided to areas that have had previous support if not in conformance with reference (c), or if major deficiencies were identified and corrective action was not initiated.

8. Detection or Suspicion of a Technical Penetration. Should a technical penetration be discovered by a command, the following actions shall be taken:

a. Do not discuss the discovery within the space where the device was found.

b. Secure the area to preclude removal of the device.

c. Do not touch the device. Make no attempts to remove the device or conduct any tests.

08 DEC 2000

d. The command shall report the details of discovery to the NCIS TSCM Program Manager (PLA: DIRNAVCRIMINSERV WASHINGTON DC//23CT//) by IMMEDIATE SECRET LIMDIS message or contact, through secure means, the NCIS TSCM program manager. In the event direct contact is not possible, the NCIS OPSCON Center, listed in enclosure (2), can locate and notify the NCIS program manager. At a minimum, the report shall include the following:

- (1) Date and time of discovery.
- (2) Area, installation, or facility involved.
- (3) Specific location within facility where the suspected device was found.
- (4) Identity of the suspected device by type (i.e. wired microphone, modified telephone, RF transmitter, etc.).
- (5) Method of discovery.
- (6) Name and any additional identifying information of the individual who discovered the device.
- (7) Best estimate as to whether any FIS was alerted to discovery.

e. No information concerning the discovery of a technical penetration shall be released to other persons or commands until authorized to do so by the Director, NCIS. No representatives of any foreign government shall be informed and no information shall be released to the public or the news media regarding a discovery without the expressed, written approval of the Director, NCIS.

f. Following any discovery of a clandestine listening device and evaluation of the circumstances described in an initial message report, NCIS TSCM Program Manager will provide instructions as to the course of action to be taken.

9. Critical Nature of Timely Reporting. The importance of timely reporting of actual or suspected technical penetrations cannot be over emphasized. In addition to the message notification addressed above, secure telecommunications via STU III (outside the area of suspected penetration) may be used to provide the most expedient notification.

08 DEC 2000

10. TSCM Personnel Selection, Training, and Equipment.

a. Personnel. TSCM operations, as a specialized counterintelligence function, require personnel with extensive investigative, electronic, and physical security skills. The Director, NCIS and the Commandant of the Marine Corps (CMC) shall staff trained TSCM personnel at a level commensurate with annual tasking, in addition to reasonable contingency surge requirements. The minimum qualifications required for entry into the TSCM field are listed in enclosure (1) to reference (a).

b. Training. All Navy and Marine Corps TSCM personnel shall receive TSCM training at a facility approved by the NCIS TSCM Program Manager to ensure survey quality and to standardize operational procedures. TSCM personnel will also undergo periodic refresher training and attend specialized courses annually to maintain proficiency, and stay abreast of new technical threats and advancing technology.

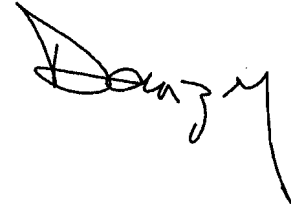
c. Equipment. TSCM equipment shall be kept current to meet the existing threat due to ever changing technology. It shall be capable of identifying, locating, neutralizing, and/or exploiting technical surveillance or collection devices targeted against the DON. TSCM equipment is constantly vulnerable to obsolescence due to continuously evolving electronic and software technologies. Per the National Policy on Technical Surveillance Countermeasures of September 16, 1997, standardized TSCM equipment shall be procured, maintained, and utilized to provide the Commander with state-of-the-art technology to obtain the required degree of confidence available to process and use sensitive information.

11. Minimize. Reports of detection or suspicion of technical penetration present a clear, time sensitive operational requirement for the use of telecommunications. A statement advising consideration of MINIMIZE shall be added to the report, as applicable, according to the means of telecommunications used. Routine requests for TSCM surveys shall be forwarded by other secure means during periods of MINIMIZE.

SECNAVINST 3850.4
08 DEC 2000

12. Report Control. The requirement contained in paragraph 7 is exempt from reports control by SECNAVINST 5214.2B and requires no report control symbol.

Richard
Richard Danzig



Distribution:
SNDL Parts 1 and 2
MARCORP PCN 71000000000 and 71000000100

TSCM REQUESTS

1. All requests for TSCM support shall be initiated as SECRET.
2. All requests shall be forwarded via registered mail to:

Director, Naval Criminal Investigative Service
Building 111, Suite 2000 ATTN: Code 23CT
716 Sicard Street SE
Washington Navy Yard, DC 20388-5386

or via Naval message to DIRNAVCRIMINVSER WASHINGTON DC//23CT//.
It is recommended that all requests be made via registered letter
vice Naval message.

3. Include the following in all requests:

- a. Complete identification of the area requiring TSCM support, to include: name of the area, room number, building number, address, location, and command if other than requester.

- b. Square footage of each space identified.

- c. Identity and secure telephone number (DSN, commercial with area code) of a command point of contact (POC) and an alternate.

- d. Clearly identify clearance requirements for TSCM support personnel. Also include the SSO's name, address, secure phone number, Naval message address, secure fax number, and any other information needed to send clearance information for TSCM personnel.

- e. Date and serial number of last TSCM report and the status of previous recommendations provided, if any.

- f. Information that may impact on the scheduling of support (i.e., date scheduled construction will commence, completion date of construction in progress, etc.). Should unexpected events occur which would interfere with a TSCM inspection after support has been scheduled, the requester shall notify the NCIS TSCM Program Manager to prevent unnecessary expenditure of manpower and travel funds.

4. POC information shall be current. If a POC changes before TSCM service is conducted, an updated request shall be submitted identifying the new POC and current contact numbers.

00 DEC 2000

TECHNICAL SUPPORT UNITS

TSCM Requests can be made to:

Director, Naval Criminal Investigative Service
Building 111, Suite 2000 ATTN: Code 23CT
716 Sicard Street SE
Washington Navy Yard, DC 20388-5386

(202) 433-3270 DSN: 288-3270
PLAD: DIRNAVCRIMINVSERV WASHINGTON DC//0023CT//

Marine Command Oversight:

Commandant of the Marine Corps (CIC)
HQMC, FB 2, Navy Annex
Washington, DC 20380-1775

(703) 614-2219/2058 DSN: 224-2219
PLAD: CMC WASHINGTON DC//C4I/CIC//

Local Inquiry/Advisory Assistance:

NCIS Technical Services Detachment, Norfolk
2340 Amphibious Drive, Suite 175
Norfolk, VA 23521-2895

(757) 363-4422 DSN: 864-4422
PLAD: NAVCRIMINVSERV TECHSVC DET NORFOLK VA//NFTV//

NCIS Technical Services Detachment, Mayport
3740 Saint Johns Bluff Road, Suite 4
Jacksonville, FL 32224

(904) 996-7881 DSN: NONE
PLAD: NAVCRIMINVSERV TECHSVC DET MAYPORT FL//MPTM//

NCIS Technical Services Detachment, Europe
PSC 819 BOX 35
FPO AE 09645-4300

34-56-823842 DSN: 727-3852/3854
NMSG PLA: NAVCRIMINVSERV TECHSVC DET ROTA SP//EUTE//
NCIS Technical Services Detachment, San Diego

Enclosure (2)

SECNAVINST 3850.4

00 DEC 2000

32640 Echo Lane
San Diego, CA 92147-5210

(619) 524-0602 DSN: 524-0602
PLAD: NAVCRIMINVSERV TECHSVC DET SAN DIEGO CA//SDTC//

NCIS Technical Services Detachment, Bangor
Land Title Professional Building, Suite L20
9657 Levin Road
Silverdale, WA 98383

(360) 396-4365 DSN: 744-4365
NMSG PLA: NAVCRIMINVSERV TECHSVC DET BANGOR WA//PSTG//

NCIS Technical Services Detachment, Hawaii
Box 132
Pearl Harbor, HI 96860-5091

(808) 474-9059 DSN: 474-9059
PLA: NAVCRIMINVSERV TECHSVC DET PEARL HARBOR HI//HITH//

USMC TSCM Inquiry/Assistance:

Commanding General
I Marine Expeditionary Force
Attn: G-2/CIHO
Camp Pendleton, CA 92055-5401

(760) 725-9121/9122 DSN: 365-9121
PLAD: CG I MEF//G-2/CIHO//

Commanding General
II Marine Expeditionary Force
Attn: G-2/CIHO
Camp Lejeune, NC 28542-0115
PSC 20115

(910) 451-8279/8185 DSN: 751-8279
PLAD: CG II MEF//G-2/CIHO//

SECNAVINST 3850.4

00 DEC 2000

Commanding General
III Marine Expeditionary Force
Attn: G-2/CIHO
FPO AP 96606

011-81-611-722-7773/7315 DSN: 622-7773
PLAD: III MEF//G-2/CIHO//

Enclosure (2)