



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
WASHINGTON, D C 20350

SECNAVINST 5500.31A
OP-009D

4 JUN 1985

SECNAV INSTRUCTION 5500.31A

From: Secretary of the Navy

Subj: TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) PROGRAM

Ref: (a) DOD Instruction 5240.5 of 23 May 84 (NOTAL)
(b) OPNAVINST 5530.14

Encl: (1) Physical Security Guidance
(2) Telephone/Miscellaneous Communications Equipment
Guidance
(3) TSCM Support Requests
(4) TSCM Support Units

1. Purpose. To address the threat of technical surveillance penetration of areas in which sensitive discussions occur. This instruction implements reference (a) which updates policies, responsibilities and procedures for the DOD Technical Surveillance Countermeasures (TSCM) Program. It contains information on the availability of TSCM support and provides guidance about technical security and the use of telephones and related equipment in sensitive discussion areas. (R)

2. Cancellation. SECNAVINST 5500.31, OPNAVINST C5500.46B and report control symbol OPNAV 5500-3 (MIN:ETAUTH).

3. Background. Historically, hostile intelligence services (HIS) 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/intercommunication systems; and radio frequency (RF) transmitters. 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. Enclosure (1) addresses physical security measures to be considered, in addition to reference (b), when establishing positive access controls for sensitive discussion areas. Enclosure (2) addresses the special threat posed by telephones and related equipment within secure discussion areas. Local security measures, implemented pursuant to the guidance set forth in enclosures (1) and (2), can be augmented with TSCM support conducted to detect the presence (A)

4 JUN 1985

of technical surveillance devices. TSCM personnel will evaluate also the space for technical and physical security vulnerabilities, and provide recommendations to eliminate any security deficiencies identified.

4. TSCM Personnel Selection and Training

a. Personnel. TSCM operations, as a specialized counter-intelligence function, require personnel with extensive investigative, electronic, and physical security skills. The minimum qualifications required for entry into the TSCM field are listed in enclosure (1) to reference (a). (A)

b. Training. All Navy and Marine Corps TSCM agents shall receive TSCM training at a facility approved by the Director, Naval Investigative Service (NIS) to ensure survey quality and to standardize operational procedures. TSCM personnel will also undergo periodic refresher training and attend specialized courses as necessary to maintain proficiency and to stay abreast of new technical penetration threats and advancing technology.

5. Policy

a. Protecting sensitive discussion areas from technical penetration is the responsibility of every commander. A comprehensive security program should 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 should include TSCM support performed by qualified investigative agents. The Director, Naval Investigative Service serves as the TSCM program manager within the Department of the Navy (DON) and is responsible for providing TSCM support, technical direction and centralized management of all TSCM efforts. The NIS is the sole activity within DON authorized to procure and use equipment for TSCM purposes, except for designated U. S. Marine Corps Counter-intelligence Teams acting under the operational control of the cognizant Marine Amphibious Force Commander and the technical direction of the Director, NIS. When not deployed in their primary tactical role, Marine Corps TSCM assets function under the cognizance of the Director, NIS, primarily for the support of Fleet Marine Force (FMF) commands and secondarily for the support of other commands. Navy and non-FMF commands shall obtain TSCM support only from or via Director, NIS. This restriction includes support for sensitive DON sponsored projects at contractor facilities. (R)

4 JUN 1985

b. A memorandum of understanding exists between the Director, NIS and counterpart agencies of the Army and Air Force to provide for cross-service TSCM support in certain overseas locations. Although Army or Air Force TSCM assets may therefore support DON activities in some instances, responsibility for approving and coordinating such support will remain with the NIS. Requests for TSCM support from Army or Air Force TSCM assets by DON activities require prior authorization from the Director, NIS.

(R)

c. TSCM surveys will be conducted in accordance with this instruction and reference (a).

(A)

6. Discussion

(R)

a. Selection of Spaces Requiring TSCM Support. Due to the cost of technical manpower, travel and equipment, reasonable selectivity must be exercised in identifying spaces to receive TSCM support. The support will be provided in accordance with the following criteria:

(A)

(1) Qualifying Spaces/Facilities. Support will be provided those spaces where discussions classified SECRET or above take place routinely and which have continuous access controls established as part of an effective security program to preclude undetected access. Guidance to achieve this objective is contained in enclosure (1).

(A)

(2) Conferences. Conferences, symposia, exhibits, clinics, conventions and meetings involving classified discussions should be held in secure spaces that have either received TSCM support previously, or would otherwise qualify for it. When such facilities are not available, one-time meetings will be supported if they are held in facilities not open to the general public, have the potential for good audio and physical security throughout the conference and when the information scheduled for discussion is classified TOP SECRET. TSCM surveys of unsecure facilities, such as base theaters, school auditoriums, unsecured classrooms, etc., can provide at best only marginal assurance that no technical penetration exists. Access by uncleared persons to such facilities before and after a classified conference, or between sessions, creates opportunities for the installation and subsequent removal of eavesdropping devices which may or may not be operative or even present during the actual survey. Adequate physical security and personnel access controls are essential; without them, a TSCM survey serves only to foster a false sense of security.

(A)

4 JUN 1985

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

(4) New/Renovated Facilities. Normally, new installations or spaces having undergone major renovations will not receive TSCM support until all construction is completed, the spaces are manned, are fully operational and security measures, as indicated here, are implemented. Pre-construction liaison with the nearest TSCM Support Unit is encouraged to ensure the standards set forth herein are understood clearly and incorporated into the construction or modification plans. TSCM support units are listed by location in enclosure (4). (A)

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

(6) Ships and Aircraft. TSCM support will not be furnished normally to naval ships or aircraft because of the low technical security threat which exists while they are deployed. (A)

b. Recurring TSCM Support. No facility will qualify automatically for routinely 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. Recurring service will be provided only if considered appropriate by the TSCM program manager whose decision will be based upon a documented threat vulnerability assessment and completed following current DoD policies. The frequency of such periodic support, where appropriate, will be determined also by the TSCM program manager based on the formalized threat assessment. Additional support may be requested when: (A)

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

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

4 JUN 1985

(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 support alone cannot substitute for good physical security and access controls.

(A)

c. Operational Security (OPSEC). TSCM services are highly specialized counterintelligence investigations and as such, are particularly vulnerable to compromise. All commands which 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 clandestine intercept device is actually in place. Should discussions concerning the pending 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 diminished greatly. For this reason, no discussion or verbal comments concerning the pending support should 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 kept to an absolute minimum. Telephone requests for TSCM support are considered compromised and are not authorized.

(A)

7. Action

a. Requests for TSCM support to augment a comprehensive security program established for each sensitive discussion area are to be submitted per paragraph 6 above, enclosure (3) and be in consonance with the following criteria:

(A)

(1) Requests for TSCM support should be submitted with as much lead time as possible. Known requirements to be supported during the next fiscal year should be submitted by 1 August. Unanticipated requirements should be submitted at least 60 days prior to the requested visit. Extenuating circumstances which require a faster response must be identified clearly and justified fully.

(2) Where feasible, commands are encouraged to consolidate the requirements of subordinate commands. Project managers and accrediting authorities responsible for the security of DON special programs and contractor facilities should also consolidate their requirements into a single annual request.

4 JUN 1985

b. Due to the sensitive nature of TSCM support, correspondence which identifies upcoming visits and dates will be kept to an absolute minimum. Requests for TSCM support will be acknowledged upon receipt. A projected calendar year (CY) quarter in which requested support can be expected will be announced. Normally, no additional correspondence will be initiated to reduce opportunities for compromise. Requesting commands will be notified by the Director, NIS should operational commitments require rescheduling of pending services. Notification will contain a new projected CY quarter for the conduct of requested services. When unforeseen circumstances arise within the requesting command which would preclude a scheduled visit, the Director, NIS should be notified immediately.

c. As an adjunct to a command's security program, TSCM investigative agents can provide TSCM threat briefings to command personnel. The briefings are classified and will be provided normally after completion of TSCM support for a facility or installation.

d. Commands will ensure that weaknesses identified as a result of TSCM services are corrected. Unless justified, TSCM support will not be provided normally to areas that have had previous support if major deficiencies were identified and no corrective action has been initiated.

e. Should a technical penetration be discovered, the following actions must be taken:

- (1) Secure the area to preclude removal of the device.
- (2) Conduct no discussions of the discovery within the space where the device was found.
- (3) Conduct no altering tests nor make any attempts at removal until a reply to the following report is received.
- (4) The command will report the discovery details to the Director, Naval Investigative Service (PLA: DIRNAVINSERV WASHINGTON DC) by Immediate SECRET message or contact the nearest TSCM Support Unit and notify DIRNAVINSERV as outlined above. TSCM Support Units are identified in enclosure (4). At a minimum, the report should include the following:

4 JUN 1985

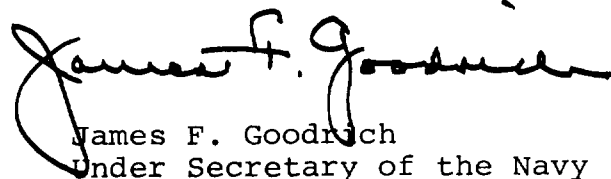
- (a) Time and date of discovery.
- (b) Area, installation or facility involved.
- (c) Specific location within facility where device was found.
- (d) Identity of device by type (i.e. wired, microphone, modified telephone, RF transmitter, etc.).
- (e) Method of discovery.
- (f) Estimate as to whether HIS was alerted to discovery.

(5) Information concerning the discovery of the technical penetration shall not be released to other persons until authorized by Director, NIS. No representatives of any foreign government shall be informed and no information will be released to the public or press regarding the discovery without Director, NIS approval.

(6) Following any discovery of a clandestine listening device and evaluation of the circumstances described by the initial message report, Director, NIS will provide technical assistance to accomplish field technical evaluation of the device.

8. Report. The reporting requirement in paragraph 7 is exempt from Reports Control by OPNAV Instruction 5214.7.

(A)



James F. Goodrich
Under Secretary of the Navy

Distribution:

SNDL	A	(Navy Department)
	21A	(Fleet Commanders in Chief)
	22A	(Fleet Commanders)
	23	(Force Commanders)
	24	(Type Commanders)
	26	(Special Commands, Groups and Units) (less 26GG)
	28	(Squadron, Division and Group Commanders Ships) (less 28G)

4 JUN 1985

Distribution (continued)

SNDL 41 (Military Sealift Commands) (less 41D and 41J)
 42 (Naval Aviation) (less 42C, 42G, 42J, 42K, 42L, 42N, 42P, 42Q, 42R, 42S, 42T, 42U, 42W, 42Y, 42Z, 42BB, 42CC, 42RR)
 50A (Unified Commands) (USCINCPAC and USCINCLANT, only)
 FA (Shore activities under CINCLANTFLT) (less FA28, FA32, and FA34)
 FB (Shore activities under CINCPACFLT) (less FB29, FB30, FB31, FB39, FB40, FB41, FB42, and FB44)
 FC (Shore activities under CINCUSNAVEUR) (less FC9 and FC11)
 FD (Shore activities under COMNAVOCEANCOM)
 FE (Shore activities under COMNAVSECGRU)
 FF (Shore activities under CNO) (less FF14, FF16, FF17, FF20, FF45, FF48, and FF49)
 FG (Shore activities under COMNAVTELCOM) (less FG9)
 FKA (Shore activities under CHNAVMAT)
 FKN (Shore activities under COMNAVFACEENG)
 FKP (Shore activities under COMNAVSEASYSYSCOM) (less FKP6, and FKP9,
 FKQ (Shore activities under COMNAVELEXSYSYSCOM)
 FKR (Shore activities under COMNAVAIRSYSYSCOM) (less FKR7 and FKR8)
 FS (Shore activities under COMNAVINTCOM)
 FT (Shore activities under CNET) (FT1, FT2 and FT5, FF42, only)
 V12 (CGMCDEC)

DCNOs and DMSOs
 MARCORPS L5 (80 copies)

Copy to:

SNDL B2A (Special agencies, staffs, boards, and committees) (NSA and DIA, only)

Stocked:

CO, NAVPUBFORMCEN
 5801 Tabor Avenue
 Phila., PA 19120-5099 (100)

4 JUN 1985

PHYSICAL SECURITY GUIDANCE

1. Physical security is the most important countermeasure to technical penetration. Access to a facility or space, or at a minimum to its immediate proximity, must be gained before a penetration can be accomplished. To understand the importance of the requirement for good access control, an appreciation of the various technical penetration techniques must be gained.

a. Wired Microphones. A technical surveillance penetration employing a wired microphone against an area with good physical security is difficult to accomplish. The task is made much simpler if the area contains unused wiring. By using existing wire runs which exit the secure perimeter, a technical penetration can be accomplished in a minimum amount of time without introducing potentially alerting additional wire.

b. Telephones and Intercommunication Systems. Modified telephone and intercommunication systems can provide a highly exploitable means of taking audio from a space without installing wiring. This type of penetration is a universal threat because spaces in which sensitive classified discussions occur contain at least one telephone or intercommunication unit. Specific guidelines for installing telephones and related communications equipment in sensitive areas to counter the threat they pose to audio security are set forth in enclosure (2). No telephones should be located in secure discussion areas, unless absolutely mission essential.

c. RF Transmitters. Recent technical penetration discoveries reveal a continued trend on the part of hostage intelligence services to employ RF transmitters. This can be accounted for by advances in technology which allow extremely small and efficient transmitters to be designed for quick installation. They are disguised often as part of an ordinary piece of office furniture. Discovery of RF transmitters is complicated further by their use of complex modulation schemes and remote deactivation capabilities which reduce the time they are detectable and conserves battery power.

d. Tape Recorders. Miniature tape recorders, which permit several hours of recording, have been improved greatly and must be considered more of a technical penetration threat than was true in the past. Should unescorted visitors who are not cleared properly have routine access to sensitive areas, such devices can be installed quickly and removed later or serviced with only minimal risk of detection.

Enclosure (1)

4 JUN 1985

e. Optical Devices. Protection from long-range optical penetrations must also be considered. Visual and optical surveillance of areas where classified material is discussed and maintained is a viable method of technically penetrating a secure area.

2. For the most part, compliance with the guidance set forth in reference (b) for providing physical security measures to protect property and material will be useful in preventing technical penetrations. Additional precautions must be applied to those areas in which classified discussions are held. While preventing adequately surreptitious entry into a room, conventional measures may do nothing to preclude removal of audio via an unprotected conduit such as an uncovered window or an air conditioning duct. Physical security protection must extend also to areas surrounding the space needing protection. By this providing a buffer area around a secure space, many audio security vulnerabilities can be avoided.

a. Audio Paths. All openings and electrical conduits which may pass usable audio to an uncontrolled area must be sealed. Ducts can be baffled acoustically to control audio which could otherwise be retrieved.

b. Excess Wiring. All conductors, including those servicing telephone, intercommunication and electrical systems, should be identified to determine if they are in use. All conductors found to be unused and excess should be removed or shorted together and grounded within the secure area to preclude their use as part of a clandestine system. Exploitation of such wiring would facilitate greatly an audio penetration.

c. Escorts. All individuals allowed into sensitive areas should be appropriately cleared or escorted. Introduction of audio devices into a space can be effected quickly, even by relatively untrained personnel. Routine access by uncleared personnel and building maintenance workers can provide ample opportunity for implanting a relatively undetectable eavesdropping device. This risk is particularly evident in overseas locations where indigenous personnel are used for these purposes. All uncleared personnel entering controlled access areas must be closely escorted by cleared personnel who have

4 JUN 1985

been briefed thoroughly on the technical penetration threat. Escorts should not only be alert to their charges removing items, but also to the possibility that a device could be left behind. Cleared personnel should be used for housekeeping services in highly sensitive locations whenever possible, especially overseas. A log of all repairs and alterations to the space should be kept to include the identities of the individual workers and repairs. This will provide a history of events occurring within an area and aid in identifying perpetrators of any possible clandestine installation found later.

3. Sound Masking. Secure areas cannot always be isolated from adjoining spaces to preclude either inadvertent or deliberate eavesdropping. Where space configurations and usage bring about this circumstance, classified conversations can be masked by an artificially introduced noise source. This can be accomplished by installing a tape system (not radio) within the security area and directing the sound produced from prerecorded tapes at those areas where eavesdropping devices might be implanted. Speakers incorporated in such a system can be installed in voids and ducts to mask sensitive conversations. To provide the intended protection, the artificial noise must be at a much higher level than the sensitive conversation. One method of obtaining this objective is to couple acoustically the artificial noise to the walls, ducts, windows, pipes, etc., using transducers. Another approach is to provide a barrier, such as a false wall, heavy floor-to-ceiling draperies or a false ceiling between the speakers and the critical discussion area, to prevent the sound cover from interfering with conversations.

4. Equipment/Furnishings. All furnishings and equipment should be mission essential and their use dedicated to the secure area. Shuttling furniture or equipment in and out of controlled areas increases the possibility of a surveillance device being hidden within them. Each item should be searched physically by a person familiar with the equipment. Equipment/furnishings introduced into the controlled space will be checked by qualified TSCM personnel during the next scheduled TSCM support to the area. Equipment which processes classified information often represents a technical security risk by emanating radio frequency (RF) signals into free space and onto existing wiring (power, telephone, intercommunications, etc.) serving a facility. Inspection and specific countermeasures for this equipment falls under the purview of the TEMPEST program as outlined in OPNAVINST C5510.93D (NOTAL). The use of non-mission essential radios and television in classified discussion areas is particularly discouraged.

4 JUN 1985

TELEPHONE/MISCELLANEOUS COMMUNICATIONS EQUIPMENT GUIDANCE

1. General. The variety and complexity of commercial telephone systems make the task of providing specific installation guidance difficult. Every installation must be examined in light of the particular environment involved. There are however, basic steps which should be followed to provide security against a technical penetration of any telephone system. The more complex a system is, the more difficult it is to prevent a penetration. The best way of eliminating the problem would be to exclude telephones from areas in which classified information is discussed and/or processed. This approach is unrealistic in the majority of situations encountered. Although it is usually possible and recommended to exclude telephones from secure conference rooms, a working area is a different matter. Communications must be provided; however, restricting the number of telephones to an absolute minimum is essential.

2. Risks. Telephones in areas where classified information is discussed or processed constitute exploitable vulnerability. Three distinct risks are involved:

a. Wiretapping. All telephone conversations are potentially subject to interception. The path followed by telephone lines often presents several terminations where conventional "wire-tapping" is possible. Also, the increased use of microwave links readily provides a means for intercepting telephone conversations through the use of RF receivers. While the latter poses the least risk of detection, a conventional wiretap approach is virtually undetectable without physically examining the entire wire path, an impossibility in today's environment. For these reasons, classified discussions are prohibited over telephone systems which are not protected by authorized encryption techniques. This restriction applies also to the discussion of classified information over intercommunications systems when such systems are integrated into the facility's telephone equipment, even if all stations are within the secure perimeter.

b. Compromising Emanations. Telephone lines may carry machine emanations from nearby equipment processing classified information to uncontrolled areas. Appropriate countermeasures to address this threat fall within the purview of the TEMPEST program as outlined in OPNAVINST C5510.93D (NOTAL).

c. Room Conversations. The potential exists for telephones to be used as part of a clandestine eavesdropping system even

Enclosure (2)

4 JUN 1985

while "on-hook" (hung-up). Telephones in the "on-hook" condition are found frequently to pass room conversations occurring in their vicinity to unprotected areas as a result of accidental or intended modification or because of a design characteristic of the telephone instrument or its associated equipment.

3. Installation Criteria. The installation of telephones within sensitive discussion areas should be in accordance with the following criteria:

a. Cable/Wire Control

(1) All telephone wires should enter the facility through one opening and each conductor should be accounted for accurately at the point of entry. The accountability will identify, through labeling or log/journal entries, the existing use of every conductor. This accountability applies to excess conductors which should be terminated at the point of entry and connected to appropriate connector blocks.

(2) When multiline telephone service is used within sensitive discussion areas, the associated Key Service Unit (KSU) should be installed within the area or in an adjacent area which is provided equal security protection. This simple step will enhance security by reducing the number of conductors that enter a facility. In this configuration, each telephone line requires only two conductors; whereas, if the KSU is situated beyond the controlled perimeter, each telephone line requires a minimum of six conductors.

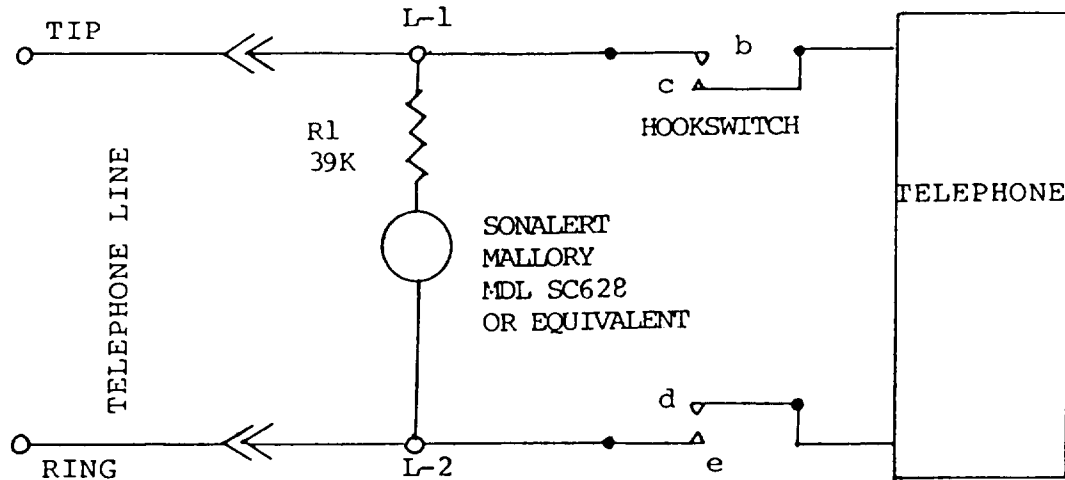
b. Isolation. Telephone instruments should be isolated from all incoming lines when not in use, i.e., in the "on-hook" condition. The recommended methods of achieving isolation are:

(1) Manual Disconnect. The simplest and most economical means of isolating a telephone instrument is to fit each instrument with a plug and jack arrangement so the telephone can be disconnected manually at all times when not in use. This method is also the most effective one, but only if the user remembers to pull the plug. Such plug and jack installations should be arranged so they are convenient to use and incorporate an audible alarm to warn users to remove the plug upon completion of calls. This audible alarm must be isolated from outgoing lines when the plug and jack are removed. Figure (1) is a diagram of the recommended method. When multiline service is required, the plug and jack can be incorporated by using a

4 JUN 1985

single line instrument and a separate key strip with a plug and jack installed between them.

SINGLE LINE TELEPHONE



<<=Plug and Jack Connections

Figure (1)

(2) Automatic Disconnect. The Western Electric Company Model 270 Automatic Telephone Disconnect Device (ATDD) is designed to provide automatic disconnection of single or two-line telephone instruments and is available only to government agencies. Although more expensive than a plug and jack arrangement, the model 270 is user transparent; i.e., it requires no action by the user to initiate or terminate a telephone call. The 270 disconnect switch is also compatible with key telephone systems when installed between a key strip and a single-line instrument in the same manner described for the manual plug and jack arrangement above. This will require the installation of a 270 switch for each telephone instrument.

(3) Optical Isolator. The U. S. intelligence community has collectively sponsored development of an optical isolator which is superior to the WECO 270 ATDD and requires no action on the part of the telephone user. The isolator is nearing the final stages of production and should be available soon. The

4 JUN 1985

isolator is designed for universal adaptability and users should realize a substantive cost savings. NIS will make an announcement when the optical isolators are available for procurement.

(4) Exception. Until optical isolators become available, use of standard multiline telephone instruments without isolation is appropriate, provided the following conditions are met:

(a) The KSU must be of U. S. manufacture and installed in accordance with paragraph 3a(2) above.

(b) The KSU should employ high security Key Telephone Unit (KTU) line cards.

(c) All instruments serviced by the KSU must be within the sensitive discussion area.

(d) The equipment must be installed and maintained by cleared U. S. personnel.

Note: This exception is offered as an interim measure with the understanding the system will be fitted with the optical isolator when it becomes available.

c. Handsets. In cases where a "hold" feature is provided, either through the use of a multiline telephone set or a separate line selector key strip, no special handset is necessary. When a "hold" feature is not available, a security handset such as the WECO G-10A, G-10B, G-10F, or equivalent is essential for protection in those situations where the instrument is left "off-hook" for short periods of time while the user obtains information, files, etc.

d. Signal. Since most standard telephone ringers have microphonic characteristics, the signaling of incoming calls within sensitive discussion areas should be accomplished in accordance with one of the following options:

(1) In facilities where the KSU is installed within the secure perimeter, no special signaling apparatus is required if the KSU includes a local ring generator and is wired for common audible signaling. Any ringer or buzzer may be used. This type of installation requires a backup power source if telephone service is required during commercial power outages.

4 JUN 1985

(2) With any ringer or buzzer modified with an approved isolator kit.

4. Intercommunication Systems. Such systems installed within sensitive discussion areas present audio security hazards similar to those related to telephone systems. The design of many intercommunication systems allow audio in their vicinity to be intercepted at any point along the connecting cable run. Unless necessary for efficient operation, intercommunication systems should not be installed in sensitive discussion areas. If determined to be essential, all components of the system, including connection cables, should remain within the established secure perimeter. Under no circumstances should intercommunication systems that employ AC power lines or RF energy as the transmission media be used.

5. Specialized Telephone Equipment. The installation of specialized telephone equipment, such as telephone answering devices and speaker phones, is discouraged within sensitive discussion areas. Such systems add to system complexity and increase the potential for undetected exploitation. In cases where operational need overrides the security ramifications, specialized telephone equipment should be installed in accordance with the provisions of paragraph 3.

6. Computerized Telephone Systems. The latest telephone systems available employ computer technology and afford a multitude of operating conveniences, but these systems are not recommended for use within sensitive discussion areas. If the use of such a system is an operational necessity, every effort should be made to ensure the entire system is installed within the discussion area or in an adjacent area which is provided equal security protection. No assurances relative to the system's security can be made unless it is so installed. Only computerized telephone switching systems compatible with the optical isolator under development should be used. Commands anticipating installing a system are encouraged to contact NIS Headquarters for an evaluation. The optical isolators should be used when they become available.

7. Secure Voice Telephones. The presence of a secure voice telephone within an uncontrolled office does not, of itself, qualify the space for TSCM support. In fact, the uncontrolled office would constitute the weak link in secure voice communications. Installation of secure voice telephones should be restricted to sensitive discussion areas afforded positive access controls which are provided periodic TSCM support. Under these conditions, the secure voice equipment can be used with greater security confidence.

4 JUN 1985

TSCM SUPPORT REQUESTS

1. All requests for TSCM support should be classified SECRET.
2. All requests should be forwarded in accordance with the following, as appropriate:
 - a. Send requests for support for Pacific area commands to the Naval Investigative Service Regional Office Pacific, Box 76, Pearl Harbor, Hawaii 96860, Attn: Technical Services Detachment Pacific (PLA for message traffic is NAVINVSEVREGOPAC PEARL HARBOR HI) with an information copy to Headquarters, Naval Investigative Service, Washington D.C. 20388, Attn: Technical Services Department. The PLA for naval message is DIRNAVINVSEV WASHINGTON DC.
 - b. Forward requests for support for Marine Corps commands following the existing editions of applicable Marine Corps orders/directives.
 - c. Send all other requests to Headquarters Naval Investigative Service.
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 the area.
 - c. Identity and telephone number (AUTOVON, commercial with area code, AUTOSEVOCOM) of the command point of contact and an alternate.
 - d. Clearance requirements for TSCM support 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 which would interfere with a TSCM inspection occur after support has been scheduled, the requester should notify the Headquarters, NIS to prevent unnecessary expenditures of manpower and travel funds.

Enclosure (3)

4 JUN 1985

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)
SUPPORT UNITSMailing Address

Headquarters
Naval Investigative Service
Washington, D. C. 20388

Commanding Officer
Naval Investigative Service
Regional Office Norfolk
Norfolk, VA 23511

Commanding Officer
Naval Investigative Service
Regional Office San Diego
P.O. Box 80667
San Diego, CA

Commanding Officer
Naval Investigative Service
Regional Office Pacific
Box 76
Pearl Harbor, HI 96860

Commanding Officer
U. S. Naval Investigative Service
Regional Office
Box 36
FPO San Francisco 96651

Team Commander
5th Counterintelligence Team
HQ Fleet Marine Force Atlantic
U. S. Naval Base
Norfolk, VA 23515

Team Commander
6th Counterintelligence Team
3rd Marine Aircraft Wing, FMF
Marine Corps Air Station El Toro
Santa Ana, CA 92709

Team Commander
9th Counterintelligence Team
III Marine Amphibious Force, FMF
FPO San Francisco 96602

Message Address

DIRNAVINSERV WASHINGTON DC

NAVINSERVREGO NORFOLK VA

NAVINSERVREGO SAN DIEGO CA

NAVINSERVREGOPAC PEARL
HARBOR HI

NAVINSERVREGO SUBIC BAY RP

CG FMFLANT
Pass to: G-2 (SCIO), 5CITCG I MAF
Pass to: G-2 (SCIO), 6CIT
INFO: CG THIRD MAWCG III MAF
Pass to: G-2 (SCIO), 9CIT

Enclosure (4)