



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 3850.4A
DUSN Policy
August 7, 2014

SECNAV INSTRUCTION 3850.4A

From: Secretary of the Navy

Subj: TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Definitions
(3) Responsibilities
(4) Technical Surveillance Countermeasures (TSCM) Requests
(5) TSCM Contact Information
(6) Qualification for Entry into TSCM Field

1. Purpose. This instruction provides policy and defines specific responsibilities for the implementation of the Department of the Navy (DON)'s Technical Surveillance Countermeasures (TSCM) program. This instruction has been revised and should be reviewed in its entirety.

2. Cancellation. SECNAVINST 3850.4.

3. Definitions. See enclosure (2).

4. Applicability. This instruction applies to the Office of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all U.S. Navy (USN), U.S. Marine Corps (USMC) installations, commands, activities, field offices, and all other organizational entities within the DON.

5. Policy. It is DON policy:

a. To ensure protection of sensitive areas from loss of classified information or technical penetration. It is the responsibility of every commander to establish a comprehensive security program for the protection of all sensitive areas. When discussions of data processing at the SECRET level or above

are held within a space on a regular basis, the security program shall include appropriately qualified TSCM support personnel.

b. That the Naval Criminal Investigative Service (NCIS) and Counterintelligence elements of the United States Marine Corps (USMC), as designated by the CMC, are hereby authorized to conduct TSCM. NCIS is designated lead agency to manage the TSCM program.

c. To eliminate foreign intelligence elements and insider threats who employ technical surveillance devices in espionage operations directed against U.S. interests, both in the U.S. and abroad. The devices employed have fallen generally into three groups: wired microphones, modified telephone or inter-communication systems, and radio frequency transmitters; however, many other methods have been used. Technology suited to clandestine surveillance applications, which is available now to virtually everyone, has exponentially increased the risk of technical surveillance penetrations.

d. That TSCM, applied effectively, can limit both the ease with which surveillance devices can be employed and their ultimate success. Enclosure (1) contains references (a) through (p) related to TSCM. References (a), (b), and (c) address physical security measures to be considered when establishing positive access controls for sensitive discussion areas. Reference (d) addresses the special considerations for telephony and related equipment within secure areas. Local security measures, implemented under the above guidance, should be augmented with TSCM support to detect the presence of technical surveillance devices.

e. To effectively manage selection of spaces requiring TSCM support. Due to the cost of manpower, travel, and specialized technical equipment, selectivity shall be exercised in identifying spaces to receive TSCM support. Support will be provided based on sensitivity, vulnerability, threat indicators, and risk management principles. Requests for TSCM functional support to facilities that are not normally used to discuss or process classified information or are open to uncontrolled access by un-cleared personnel shall be approved only in extraordinary circumstances. TSCM of such facilities have proven counterproductive by giving the occupant or occupants a false sense of security and by using limited TSCM assets that

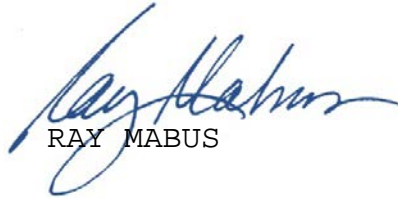
could be used more productively in other, more sensitive facilities. If approved, the requestor must make arrangements to maintain the security of the area during the TSCM and after its completion. Additional guidance has been provided in enclosures (1) through (6) of this instruction.

f. That TSCM support shall be requested and conducted per references (e), (f) through (j) per enclosures (3) through (5).

5. Responsibilities. See enclosure (3).

6. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

7. Forms and Reports. The requirements contained in this instruction are exempt from reports control and require no report control symbol.



RAY MABUS

Distribution:

Electronic only, via Department of the Navy Issuances Web site
<http://doni.documentservices.dla.mil/>

REFERENCES

- (a) Intelligence Community Directive (ICD) 700 of 7 June 2012
- (b) Intelligence Community Directive (ICD) 705 of 26 May 2010
- (c) SECNAVINST 5510.36A of 06 October 06
- (d) Telephone Security Guides (TSG) of June 2006, Not Available (NOTAL)
- (e) Intelligence Community Directive (ICD) 702 of 18 February 2008
- (f) U.S., Director of Central Intelligence Directive Procedural Guide No. 1 - Requirements for Reporting and Testing Technical Surveillance Penetrations, U.S. DCI, August 1984
- (g) U.S. Director of Central Intelligence, Director of Central Intelligence Directive Procedural Guide No. 2 - Requirements for Reporting and Testing Hazards, U.S. DCI, August 1984
- (h) U.S. Director of Central Intelligence, Director of Central Intelligence Directive Procedural Guide No. 3 - Guidance for Conducting Audio Countermeasures Surveys, U.S. DCI, August 1984
- (i) DoD S-5240.05-M-1 of 30 April 2007
- (j) DoD S-5240.05-M-2 of 13 November 2007 (NOTAL)
- (k) SECNAV M-5510.36
- (l) DoD Instruction C-5240.08 of 28 November 2011
- (m) Quad Service MOU USAF OSI, USA G2X, NCIS, and USMC DIRINT, 22 October 2012(NOTAL)
- (n) DoD Instruction 5240.05 of 3 April 2014
- (o) Joint Air Force - Army - Navy (JAFAN) 6/9 dated 23 March 2004
- (p) Marine Corps Order (MCO) 5511.20 of 25 March 1999

DEFINITIONS

1. Technical Surveillance Countermeasures (TSCM). Techniques and measures to detect, neutralize, and/or exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information.
2. TSCM Activity. Any activity conducted by TSCM personnel employing TSCM techniques, tactics, and procedures (TTP). TSCM activities may or may not involve the employment of TSCM equipment, including equipment not specific to TSCM but that is employed specifically for TSCM purposes.
3. Fully-instrumented TSCM Activity. A TSCM activity that utilizes the full range of TSCM equipment and TTPs.
4. Limited-scope TSCM Activity. A TSCM activity that does not meet the definition of "fully-instrumented". Examples include in-conference monitoring and pre-construction advice and assistance.
5. TSCM Survey. A generic term referring to a fully-instrumented TSCM evaluation of a fixed facility to validate the presence or absence of adversarial technical surveillance. A TSCM survey also identifies technical and physical vulnerabilities that could facilitate a technical surveillance operation and provides recommendations for corrective actions.

RESPONSIBILITIES

1. The Director, NCIS (DIRNCIS) shall designate a TSCM Program Manager to coordinate and de-conflict activities within the DON. The DON TSCM Program Manager is responsible for providing the technical direction and centralized oversight of all NCIS TSCM assets and their utilization. NCIS TSCM activities shall be primarily directed towards USN and NCIS requirements. NCIS TSCM elements may provide TSCM support external to the USN and NCIS per reference (n).
2. The USMC Director of Intelligence (DIRINT) shall designate a USMC TSCM Program Manager. The USMC TSCM Program Manager is responsible for providing technical direction and centralized oversight of USMC TSCM assets. USMC TSCM elements primarily support the USMC. USMC TSCM elements may provide TSCM support external to the USMC in accordance with reference (n). The DIRINT shall develop and implement policies and procedures for the conduct of TSCM within the USMC.
3. NCIS and USMC TSCM programs are the sole activities within DON authorized to employ equipment for TSCM purposes.
4. To protect sensitive operations, all support requests and correspondence shall be directly conveyed between the DON TSCM Program Manager and the USMC TSCM Program Manager.

TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) REQUESTS

1. Program Sensitivity. It is incumbent upon every commander to maintain the security integrity of sensitive compartmented information facilities and facilities where special access programs are discussed and to practice operational security regarding the use of TSCM activity. TSCM functional support alone is not a substitute for required physical security measures.

2. Requesting TSCM Support

a. Requests for TSCM support shall contain, at a minimum, the information described in this enclosure. Per reference (l), the supporting TSCM organization, e.g., NCIS or USMC TSCM element, shall prioritize requests for TSCM support and shall only accept requests for those facilities, or categories of facilities, that are determined to be probable and feasible targets for technical espionage or exploitation based on the value of the information processed in those facilities.

b. Navy activities shall submit written requests for TSCM support to the DON TSCM Program Manager directly or through the supporting TSCM office. This includes support for sensitive DON-sponsored projects at contractor facilities.

c. Marine Corps activities shall submit requests for TSCM support to the USMC TSCM Program Manager per procedures established by the DIRINT and in accordance with reference (p).

d. A Quad-Service Memorandum of Understanding, per reference (m), allows for cross-service TSCM support. For Navy support requests, the responsibility for receiving, approving, requesting, and coordinating such support remains with the DON TSCM Program Manager and the USMC TSCM Program Manager for USMC support requests.

e. Requests for TSCM functional support to facilities that are not normally used to discuss or process classified information or are open to uncontrolled access by un-cleared personnel shall be approved only in extraordinary circumstances. If approved, the requestor must make arrangements to maintain the security of the area during the TSCM and after its completion. TSCM 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) All requests for TSCM support shall be in writing, signed by the commanding officer or authorized designee, and shall be designated at a minimum SECRET or commensurate with the appropriate higher security classification level, per references (b) and (o).

(2) All signed requests shall be submitted via registered U.S. Mail, or if authorized, via the appropriately classified computer network.

(3) Include the following in all requests, at a minimum:

(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) A secure telephone number (DSN, commercial with area code) outside of the area of inspection, for the command's primary and alternate point of contact (POC).

(d) Clearly identify clearance requirements for TSCM support personnel. Also include the Special Security Officer's (SSO) name, address, secure phone number, secure fax number, and any other information needed to send clearance information for TSCM personnel.

(e) Date and serial or report number of the last TSCM report and the status of previous remediation recommendations, if any.

(f) Information that may impact the scheduling of TSCM support, such as the date scheduled construction will commence and completion date. To prevent unnecessary expenditure of manpower and travel funds, the TSCM Program Managers shall be notified if any unexpected events occur which will interfere with the TSCM inspection.

3. Qualifying Spaces/Facilities. Depending on manpower and equipment availability, support will be provided to sensitive compartmented information facilities and facilities where special access programs are discussed, in compliance with reference (b) and (p), respectively. TSCM support shall be provided to certain spaces where discussions or processing of information, classified SECRET or above, routinely take place. Continuous access controls need to be established as part of an effective security program to preclude undetected access. Guidance to achieve this objective is contained in reference (b).

a. Conferences. Per reference (o), classified meetings may only be held at an approved U.S. Government facility or a cleared DoD contractor facility with an appropriate facility security clearance where adequate physical security and procedural controls have been approved. Classified meetings may not be held at hotels, conference centers or any other uncleared venue. TSCM servicing organizations may approve requests on a case-by-case basis for facilities that do not meet these requirements. For facilities that are not open to the general public and have the potential for good audio and physical security, access control to the facility needs to be established prior to the TSCM support, throughout the conference, and continued thereafter.

b. Flag Offices/Residences. TSCM of flag offices and permanent quarters may be provided despite minimal security provisions, if doing so will not impact the completion of primary facility TSCMs. Priority consideration shall be given to locations outside the United States where the Foreign Intelligence Services threat is greatest. It should be noted that TSCM functional support conducted under such conditions have no residual value and it cannot be assumed that after the TSCM such spaces will continue to be safe for sensitive discussions.

c. New/Renovated Facilities. New installations or spaces having undergone major renovations will not receive full TSCM support until all construction is completed, the spaces are manned, fully operational, and security measures are implemented. Written requests for direct pre-construction liaison is strongly encouraged to ensure proper security standards. Submit requests for TSCM support in accordance with

policies and procedures established by the DIRNCIS and DIRINT and ensure they are clearly articulated, understood and incorporated into the construction or modification plans. A request for pre-construction support does not constitute a request for TSCM support. A written request for TSCM support, as set forth in this enclosure, must be made once the facility renovations have been completed.

d. Automobiles. TSCM support for automobiles shall 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 continually maintained by cleared personnel.

e. Ships and Aircraft. TSCM support shall not be furnished to naval ships or aircraft unless justified by extraordinary circumstances.

f. 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 inspect both logical and physical components of computers, computer networks and telephony systems to identify technical compromise or surreptitious extraction of information from the area. Protective measures may be recommended to enhance the protection of digital information from threats of computer network or telecommunication system intrusion and exploitation.

g. Optionally Selected Facilities. In the interest of protecting sensitive and/or classified information, facilities may be designated as candidates for TSCM support by the TSCM Program Managers. In such cases, the selected facility shall be notified by the respective TSCM Program Manager prior to the TSCM support in order to coordinate and secure the required authorizations to complete the support. Per applicable policies, TSCM program coordination with the offices of the CNO or CMC may be required to de-conflict command and control issues.

4. Recurring TSCM Support. No facility shall automatically qualify for recurring TSCM service. The results are considered valid as long as the security integrity of the facility is maintained. Additional support may be requested when:

a. There is documented evidence to suggest an area has been technically penetrated or compromised.

b. Extensive construction, renovation or structural modifications have required unescorted access by uncleared individuals.

c. Unauthorized personnel have gained uncontrolled or unescorted access to the secure area.

5. Operational Security (OPSEC):

a. In the interest of both good security and economy of resources, it is incumbent upon commanders to maintain the security integrity of sensitive facilities and to keep the use of this contingency to a minimum. TSCM functional support alone cannot substitute for required physical security measures.

b. TSCM services are highly specialized counterintelligence activities, and as such, are particularly vulnerable to compromise. During the provisions of TSCM administration, planning or services, OPSEC measures shall be implemented by TSCM staff and commands receiving the support to ensure the success of the TSCM support effort. Discussion or verbal comments concerning the pending TSCM support are not permitted within the spaces of concern. Written requests for TSCM service shall be classified SECRET at a minimum and follow reference (m). The number of persons apprised shall be kept to an absolute minimum. Non-secure telephonic contact shall not be made from the area for which the request is being made. Non-secure telephonic requests for TSCM support shall be considered compromising and are prohibited.

c. Written requests for TSCM support shall be submitted to the supporting TSCM organization for review, determination of validity, approval and scheduling. Due to manpower constraints, routine requests for TSCM support may not be fulfilled as requests for support will be handled on threat based, prioritized and then first-come, first-serve basis. A request for TSCM support shall remain valid for a period of two years upon receipt. Unanticipated requirements shall be submitted immediately and documentation of extenuating circumstances which require a faster response shall be clearly identified and

fully justified within the request. Requests shall be submitted as stated in paragraph 2 of this enclosure.

d. Due to the sensitive nature of TSCM support, communications or discussions that identify TSCM locations, dates, or TSCM staff shall be kept to an absolute minimum and commensurate with the security classification level of the TSCM request. 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 60 calendar days prior to arrival of the TSCM team. Normally, minimal correspondence will be initiated to reduce opportunities for compromise. If there is a change to the facility's status, POC, or an unforeseen circumstance arises within the requesting command which would preclude a scheduled TSCM visit, the supporting TSCM organization shall be notified immediately. Failure to do so may result in the cancelation of the scheduled TSCM support.

e. TSCM personnel shall evaluate the applicable spaces for technical and physical security vulnerabilities and when observed, provide recommendations to eliminate any security deficiencies identified.

f. Commands shall ensure, via a written response as per reference (o) that remediation actions for all weaknesses identified as a result of the TSCM process are documented. Unless otherwise justified, TSCM support shall not be provided to areas that have had previous TSCM support if not in conformance with reference (b) or if major deficiencies were previously identified and corrective actions were not initiated.

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

a. Requests for TSCM support shall contain, at a minimum, the information in this enclosure. Following reference (o), the supporting TSCM organization, e.g., NCIS or USMC TSCM element, shall prioritize requests for TSCM support and shall only accept requests for those facilities, or categories of facilities, that are determined to be probable and feasible targets for technical espionage or exploitation based on the value of the information processed in those facilities.

b. Navy activities shall submit requests for TSCM support to the DON TSCM Program Manager. This includes support for sensitive DON-sponsored projects at contractor facilities.

c. Marine Corps activities shall submit requests for TSCM support to the USMC TSCM Program Manager and follow policies and procedures established by the DIRINT.

7. Detection or Suspicion of a Technical Penetration. Should a confirmed or suspected technical penetration be discovered, the following actions shall be taken:

a. No discussion of the discovery shall take place within the space where the device was found.

b. The area shall be secured to preclude removal of the device.

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

d. Navy Commands shall immediately report the details of discovery to the DON TSCM Program Manager through secure means. In the event direct contact is not possible, the NCIS Multiple Threat Alert Center (MTAC), listed in enclosure (5), shall be contacted and will locate and notify the DON TSCM Program Manager. Marine Corps Commands shall immediately report the details of discovery to the USMC TSCM Program Manager through secure means and carefully follow policies established by the DIRINT in accordance with Marine Corps Order 5511.20 reference (p). The USMC TSCM Program Manager shall subsequently notify the DON TSCM Program Manager. At a minimum, the reporting shall include the following:

(1) Date and time of discovery.

(2) Area, installation, or facility involved.

(3) Specific location within the facility where the suspected device was found.

(4) Identity of the suspected device by type, i.e., wired microphone, modified telephone, radio frequency 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 foreign intelligence entity (FIE) was alerted to discovery.

e. The command shall maintain as normal an operational tempo as possible so the discovery is not realized.

f. The DON and USMC TSCM Program Managers may coordinate with appropriate DoD and national counterintelligence and intelligence entities as necessary to affect an appropriate response to a confirmed or suspected technical penetration. No release of information concerning the discovery of a technical penetration shall occur without the authorization of the Deputy Under Secretary of Defense for Intelligence and in coordination with the Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration. In all cases, the USMC TSCM Program Manager shall coordinate any release of information with the DON TSCM Program Manager to ensure the integrity and viability of potential investigative activities.

g. Following any discovery of a clandestine surveillance device, the supporting TSCM organization Program Manager will provide instructions as to the course of action to be taken.

8. Critical Nature of Timely Reporting. Secured telephony and or computer network, e.g., Secure Internet Protocol Router Network (SIPRNET), outside the area of suspected penetration may be used to provide the most expedient notification.

9. TSCM Personnel Selection, Training, and Equipment

a. Personnel. The minimum qualifications, selection, and training required for entry into the TSCM field are listed in enclosure (6).

b. Equipment. TSCM equipment shall be kept current to meet existing threats due to ever-changing technology. It is essential to provide commanders a high degree of confidence to process and use sensitive information. Standardized TSCM equipment shall be procured, maintained, and utilized with

state-of-the-art technology per the National Policy on Technical Surveillance Countermeasures of September 16, 1997.

10. Minimize. It is paramount to immediately report detection or suspicion of technical penetration. A statement within the report advising minimal distribution shall also be added. Routine requests for TSCM functional support shall be forwarded via secure means during periods of MINIMIZE.

TSCM CONTACT INFORMATION

1. Submit TSCM requests to:

a. NCIS:

Director, Naval Criminal Investigative Service
ATTN: Code 2G02
27130 Telegraph Road
Quantico, VA 22134
Phone: (571) 305-9652 DSN: (315) 240-9652
SIPR Email: NCISHQ-TSCM@NCIS.NAVY.SMIL.MIL

b. Multiple Threat Alert Center (MTAC)

- Commercial Phone: 571-305-4900
- Toll Free: 1-800-278-9914
- Secure: 571-305-4778 (STE); 918-5544 (DVOIP)
- SCI TANDBERG: 912-3845
- SECRET TANDBERG: 571-4777
E-mail:
(SIPR) MTACWATCH@NCIS.NAVY.SMIL.MIL
(JWICS) MTACWATCH@NCIS.IC.GOV

2. Classified Computer Networks TSCM contact information can be found on the NCIS and USMC homepages.

a. [HTTP://WWW.NCIS.NAVY.SMIL.MIL/DISPLAYS/TSCM/INDEX.HTM](http://WWW.NCIS.NAVY.SMIL.MIL/DISPLAYS/TSCM/INDEX.HTM)

b. [HTTP://WWW.MCIA.USMC.SMIL.MIL](http://WWW.MCIA.USMC.SMIL.MIL)

QUALIFICATION FOR ENTRY INTO TSCM FIELD

1. TSCM is a specialized counterintelligence function and requires personnel with extensive electronic and physical security skills. The Director NCIS, CNO and the CMC shall coordinate the appropriate funding and staffing of trained and equipped TSCM personnel at a level commensurate with annual tasking requirements, in addition to reasonable contingency surge needs. The minimum qualifications required for entry into the TSCM field are listed in reference (f).

2. All NCIS and Marine Corps TSCM personnel shall be certified to conduct TSCM activities per reference (f). TSCM personnel shall undergo annual TSCM training commensurate with policies, attend specialized courses to maintain proficiency, and stay abreast of new technical threats and advancing technology.

3. The minimum qualifications required for entry into the TSCM field are as follows:

a. Education. At a minimum, the candidate must have a high school diploma or equivalent and must have completed a course in electronics fundamentals.

b. Experience. It is highly desirable that candidates have experience such as electronics, avionics, telephone systems operations and maintenance, information systems operations and maintenance, and/or alarm systems operation and maintenance.

c. Security Clearance. TOP SECRET, eligible for access to Sensitive Compartmented Information.

d. Grade. E-5 or higher, or a civilian grade as determined by the authorized TSCM organization.

e. Age. Twenty-one years or older.

f. Physical. The TSCM applicant shall meet physical standards set forth by the DON and USMC TSCM organizations. The minimum requirements are:

(1) Hearing acuity tests results per audiometer test not to exceed 30 decibels (A.S.A. or equivalent I.S.O.) in either

ear in the 500, 1000, and 2000 Hz ranges. Applicants must be able to hear the whispered voice at 15 feet with each ear without the use of a hearing aid.

(2) Vision must be a minimum of 20/30 in one eye and 20/20 in the other eye, distant and near, through normal vision or corrective measures.

(3) Color perception test results, employing the pseudo-isochromatic plates for testing color perception, not to exceed four incorrect identifications out of fourteen test plates.

(4) Free from any physical problems which materially hinder manual dexterity. Applicant must have normal range of motion in all extremities.

g. A complete medical examination showing no medical reason for the applicant to be unable to complete rigorous training and performance of duties to include the following:

(1) Ability to lift forty pounds overhead, using both arms.

(2) Ability to carry forty pounds in a manner similar to carrying a suitcase.

(3) Ability to climb a six-foot ladder.

(4) Ability to crawl beneath a three-foot barrier.