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 3850.4A.

3. **Definitions.** See enclosure (2).

4. **Applicability.** This instruction applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), the Naval Criminal Investigative Service (NCIS), 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. That TSCM will be used to protect against unauthorized or inadvertent access or removal of classified Department of Defense (DoD) information through technical surveillance and associated devices, technologies, and hazards. It is the responsibility of every commander to establish a comprehensive security program for the protection of sensitive information. TSCM activities may be conducted anywhere classified DoD
information is discussed or processed. This includes, but is not limited to, vehicles and structures owned or leased by commercial or government entities to include cleared defense contractors (CDC). When classified discussions and/or processing occur within a space on a regular basis, the security program shall include TSCM support in line with this instruction and in accordance with references (a) through (w). TSCM activities shall include support to DON Critical Information and Infrastructure Protection (CIP); Technical Security Assurance; Research, Development, and Acquisition (RDA); Insider Threat; Special Access Programs (SAP); and appropriate CDC. To protect sensitive areas against 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 and/or data processing, at the SECRET level or above, occur within a space on a regular basis, the security program shall include TSCM support in line with this instruction and in accordance with references (a) through (r). TSCM activities shall include support to DON CIP; Technical Security Assurance; RDA; Insider Threat; SAP; and appropriate CDC.

b. The USMC and NCIS are the sole activities within the DON authorized to employ equipment for TSCM purposes. All TSCM activities within the DON will be coordinated with the DON TSCM program coordinator, pursuant to references (i), (v), and (w).

c. 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 (r) related to TSCM. Local security measures should be augmented with TSCM support to detect the presence of technical surveillance devices.

d. 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. Additional guidance has been provided in enclosures (1) through (4) of this instruction.
e. That TSCM support shall be requested and conducted per references (e) through (l) per enclosures (3) and (4).

f. To protect sensitive operations, all support requests and correspondence shall be directly conveyed to the NCIS and USMC TSCM Program Managers, as appropriate.

g. Upon discovery of suspected technical surveillance by any DON or DON supported component, the supporting security manager and the NCIS TSCM Program Manager will be immediately notified.

6. Responsibilities. See enclosure (3).

7. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

8. Reports. The reporting requirements contained in enclosure (3), paragraph 5 and enclosure (4) paragraph 7d are exempt from information collection control, per reference (y), Part IV, paragraph 7o.

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni.
REFERENCES

(a) Intelligence Community Directive (ICD) 700 of 7 June 2012
(b) Intelligence Community Directive (ICD) 705 of 26 May 2010
(c) SECNAVINST 5510.36
(d) Telephone Security Guides (TSG) of Jun 2006 (NOTAL)
(e) Intelligence Community Directive (ICD) 702 of 18 Feb 2008
(f) U.S., Director of Central Intelligence Directive
Procedural Guide No. 1 - Requirements for Reporting and
Testing Technical Surveillance Penetraions, U.S. DCI, Aug
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,
Aug 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, Aug 1984
(i) DoD Manual S-5240.05, The Conduct of Technical Surveillance
Countermeasures (TSCM) of 14 March 2016 (NOTAL)
(j) DoD Manual 5240.01, Procedures Governing the Conduct of DoD
Intelligence Activities of 8 August 2016
(k) SECNAV M-5510.36
(l) DoD Instruction C-5240.08 of 28 November 2011 (NOTAL)
(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) DoD Technical Surveillance Countermeasures (TSCM) Security
Classification Guide, Ver. 1.0 of 19 July 2016
(p) DoD Instruction S-5240.23 of 16 October 2013 (NOTAL)
(q) Joint Air Force - Army - Navy (JAFAN) 6/9 dated 23 Mar
2004
(r) MCO 5511.20
(s) SECNAVINST 3850.2E
(t) DoD Instruction 5240.16 of 27 August 2012
(u) DoD Instruction 5240.10 of 5 October 2011
(v) SECNAVINST 5430.7R
(w) SECNAVINST 5430.107
(x) SECNAVINST 5000.34F
(y) SECNAV M-5214.1

Enclosure (1)
DEFINITIONS

1. **TSCM.** Techniques to deter, neutralize, and exploit technical surveillance technologies and hazards that permit the unauthorized access to or removal of 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.

6. **Surveillance Device.** A piece of equipment or mechanism used to gain unauthorized access to and removal of information.

7. **Technical Surveillance.** The use of optical, audio, or electronic monitoring devices or systems to surreptitiously collect information.

8. **Technical Threat Analysis.** A continual process of compiling and examining information on technical surveillance activities against personnel, information, operations, and resources.

9. **TSCM Equipment.** Equipment or mechanisms used to identify the presence of surveillance devices. TSCM includes general purpose, specialized, or fabricated equipment to determine the existence and capability of surveillance devices.
10. **TSCM Practitioner.** An individual trained and certified to conduct all TSCM activities within the DON.

11. **TSCM Technician.** An individual trained to perform limited TSCM activities under the oversight of a TSCM practitioner.

12. **Coordination.** For the purposes of this instruction, coordination is defined as a prerequisite to de-confliction; advising of intent, sharing details of execution, ensuring mutual support, and providing after-action information.

13. **De-confliction.** For the purposes of this instruction, the process of sharing information regarding collection between multiple agencies to eliminate potential duplication of effort, multiple unintended use of the same source, or circular reporting.
RESPONSIBILITIES

1. **SECNAV** is responsible for, and maintains oversight over, all DON TSCM activities.

2. **The Under Secretary of the Navy (UNSECNAV)** shall:
   a. Provide TSCM policy oversight.
   b. When requested, provide appropriate agencies with TSCM budgetary submissions and relevant information in support of TSCM reviews.

3. **The Deputy Under Secretary of the Navy** shall:
   a. Ensure coordination across the DON and assist the UNSECNAV with oversight responsibilities.
   b. Under the direction and control of UNSECNAV, oversee TSCM activities, programs, and resources to ensure compliance with national, DoD, and DON TSCM and CI policies.
   c. Coordinate with the key stakeholders on the DON position for forums and groups with USN and USMC TSCM interests.

4. **The CNO** shall:
   a. Recommend TSCM policy and guidance changes to the UNSECNAV.
   b. Ensure TSCM teams have full, and unfettered, access to necessary facilities, spaces, equipment, and physical and logical networks needed to perform their assigned functions.
   c. Provide annual USN TSCM priorities list to the NCIS TSCM Program Manager, and Director, Naval Criminal Investigative Service (DIRNCIS), in order to support USN CI activities and requirements at USN Bases, Stations, and Installations.

5. **The CMC** shall:
   a. Recommend TSCM policy and guidance changes to the UNSECNAV.
b. Ensure TSCM teams have full, and unfettered, access to necessary facilities, spaces, equipment, and physical and logical networks needed to perform their assigned functions.

c. Provide notification and reports of significant activity, or findings, to the UNSECNAV, in coordination with NCIS via reference (v).

d. Coordinate with CNO, and the NCIS TSCM Program Manager, on USN CI program TSCM priorities.

e. Appoint a TSCM Program Manager for the USMC, who shall:

   (1) Be TSCM certified in accordance with references (n) through (r), and this instruction.

   (2) Prioritize, coordinate and de-conflict TSCM activities across the USMC and with the NCIS TSCM Program Manager.

   (3) Ensure that the USMC TSCM program is in compliance with this instruction and the policy and direction of references (a) through (x).

   (4) Develop, train, and utilize TSCM analysts to provide a facility technical threat analysis to determine if a requested TSCM, or proactively initiated TSCM support to a location or facility, is warranted. Facilities may not automatically receive a recurrent TSCM.

   (5) Provide TSCM support to external organizations per references (m) and (n) as directed.

   (6) Upon receipt of a TSCM request, notify the customer of approval or disapproval with written justification.

   (7) Approve requests for assessment of facilities or categories of facilities that are probable and feasible targets for technical surveillance or exploitation based on the facility technical threat analysis.
(8) No later than 30 business days after completion of a TSCM, provide a final report to the customer, facility, or other facility accreditation authority.

(9) Record TSCM reporting and feedback into approved CI information.

(10) Develop the capability of CI-focused TSCM targeting using a risk-based approach with the goal of identifying and exploiting technical collection efforts targeting USMC interests.

(11) Provide technical direction and centralized oversight of USMC TSCM assets.

(12) Represent the USMC at the Integrated Management Group (IMG) and other functionally related working groups and forums.

6. The DIRNCIS shall:

   a. As the Senior Official for Counterintelligence for the DON, act as the DON Senior Agency Official for TSCM and ensure TSCM activities are properly coordinated with other elements of the DON CI program.

   b. Designate a DON TSCM program coordinator, who shall:

      (1) Be TSCM certified in accordance with reference (n) and this instruction.

      (2) Coordinate and de-conflict TSCM activities within the DON.

      (3) Ensure that all DON TSCM programs are in compliance with policy and direction of references (a) through (x).

   c. Recommend TSCM policy and guidance changes to the UNSECNAV.

   d. Provide TSCM support to external organizations per references (m), (n), and (u) as directed.
e. Provide notification and reports of significant activity, or findings, to the UNSECNAV.

f. Appoint a NCIS TSCM Program Manager, or an individual to assume the responsibilities, for USN assets and equities, who shall:

(1) Be TSCM certified in accordance with reference (n) and this instruction.

(2) Prioritize, coordinate, and de-conflict TSCM activities across the USN and NCIS.

(3) Develop, train, and utilize TSCM analysts to provide a facility technical threat analysis to determine if a requested TSCM, or proactively initiated TSCM support to a location or facility, is warranted. Facilities may not automatically receive a recurrent TSCM.

(4) Upon receipt of a TSCM request, notify the customer of approval or disapproval with written justification.

(5) Approve requests for assessment of facilities or categories of facilities that are probable and feasible targets for technical surveillance or exploitation based on the facility technical threat analysis.

(6) No later than 30 business days after completion of a TSCM, provide a final report to the customer, facility, or other facility accreditation authority.

(7) Record TSCM reporting and feedback into the DoD approved CI information reporting system of record.

(8) Develop the capability of CI-focused TSCM targeting using a risk-based approach with the goal of identifying and exploiting technical collection efforts targeting USN and NCIS interests.

(9) Provide technical direction and centralized oversight of all NCIS TSCM assets and their utilization.
(10) Coordinate with the Deputy Director of Naval Intelligence (DDNI), via the CNO, for the USN TSCM priorities list and biannual operational.

(11) Represent the USN at the IMG and other functionally related working groups and forums.
TECHNICAL SURVEILLANCE COUNTERMEASURES REQUESTS

1. Program Sensitivity. It is incumbent upon every commander to maintain the security integrity of sensitive compartmented informational 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. USN activities shall submit written requests for TSCM support to the NCIS TSCM Program Manager directly or through the supporting TSCM office. This includes support for sensitive DON-sponsored projects at contractor facilities.

   c. USMC activities shall submit requests for TSCM support to the USMC TSCM Program Manager per procedures established by the USMC Director of Intelligence (DIRINT) and in accordance with reference (r).

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

   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 are not meant to give the
occupant or occupants a false sense of security. The following additional guidance applies:

(1) All requests for TSCM support shall be in writing and signed by the commanding officer or authorized designee and shall be classified, at a minimum SECRET or, commensurate with the appropriate security classification level, per references (b) and (o).

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

(3) Include the following, at a minimum, 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) An unsecure and secure telephone number outside of the area of inspection, for the command’s primary and alternate point of contact (POC).

(d) Clearly identify security clearance requirements for TSCM support personnel. Also include the Special Security Officer’s name, address, unsecure/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 scheduled construction. To prevent unnecessary expenditure of manpower and travel funds, the TSCM program manager 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 facility and facilities where SAPs are discussed, in compliance with references (b) and (r) respectively. TSCM support shall be provided to spaces where discussions or processing of information, classified SECRET or above, routinely takes 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 (q), 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 U.S. 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/or DIRINT
(as appropriate) 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 may be furnished to USN and USMC ships, aircraft, or other assets if the requested support meets program justification and prioritization thresholds.

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 shall 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 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, thereafter updated requests will be coordinated by
the TSCM program. Unanticipated requirements shall be submitted immediately and the 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 90 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. TSCM personnel and equipment shall be granted unfettered physical and logical access to all areas within the requested location, including information technology networks and telephone systems within facilities or commands, and all areas that house network infrastructure and cable runs, during the conduct of a TSCM per reference (n).

f. Commands shall ensure, via a written response as per reference (n), 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 enclosure (4). Following reference (o), the supporting TSCM organization 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. USN activities shall submit requests for TSCM support to the NCIS TSCM Program Manager. This includes support for sensitive DON-sponsored projects at contractor facilities.

c. USMC 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. USN Commands shall immediately report the details of discovery to the NCIS TSCM Program Manager through secure means. In the event direct contact is not possible, the NCIS Multiple Threat Alert Center shall be contacted and will locate and notify the NCIS TSCM Program Manager. USMC 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 reference (r). The USMC TSCM Program Manager shall immediately notify NCIS, the DON Military Department Counterintelligence Organization (MDCO), and subsequently notify the NCIS 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 was alerted to discovery.

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

f. In accordance with reference (n), NCIS, as the DON MDCO, 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 Director for Intelligence (Intelligence and Security) in coordination with the Deputy Under Secretary of the Navy. In all cases, the USMC and NCIS TSCM Program Managers shall coordinate all relevant information 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, outside the area of suspected penetration may be used to provide the most expedient notification.
9. **TSCM Personnel, Training, and Equipment**

   a. Personnel. The minimum qualifications, selection, and training required for entry into the TSCM field are listed in enclosure (5). TSCM practitioners and technicians shall be appropriately vetted, trained, and supported in accordance with references (a) through (r) and enclosure (5).

   b. Equipment. TSCM equipment shall be kept current to meet the existing threats due to ever-changing technology. It is essential to provide commanders a high degree of confidence to process and use sensitive information. Adequate supplies of 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 be added. Routine requests for TSCM functional support shall be forwarded by other secure means during periods of MINIMIZE.
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 apply the appropriate funding and staffing of trained and equipped TSCM personnel at levels 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 references (f) and (n).

2. All NCIS and USMC TSCM personnel shall be certified to conduct TSCM activities per references (f) and (n). 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.