Department of Defense
INSTRUCTION

NUMBER 5240.05
February 22, 2006

USD(I)

SUBJECT: Technical Surveillance Countermeasures (TSCM) Program

References: (a) DoD Instruction 5240.5, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," May 23, 1984 (hereby canceled)
(b) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997
(c) DoD Instruction 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," May 14, 2004
(d) DoD Instruction 5240.16, "DoD Counterintelligence (CI) Functional Services," May 21, 2005
(e) through (n), see Enclosure 1

1. PURPOSE

This Instruction:

1.1. Reissues Reference (a) and implements Reference (b) as it pertains to the DoD TSCM program.

1.2. Defines the role of TSCM as one of the counterintelligence (CI) functional services, References (c) and (d).

1.3. Defines the responsibilities of the Director, DoD Counterintelligence Field Activity (DoD CIFA) and the Director, National Security Agency (NSA)/Central Security Service (CSS) in the DoD TSCM program.

2. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the “DoD Components”).

3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. TSCM shall be conducted in the Department of Defense using 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, pursuant to DoD Directive 5240.2 (Reference (b)).

4.2. A designated lead agency shall provide TSCM support to the DoD organizations that lack an organic TSCM capability. The lead agencies are listed in Enclosure 3. Only DoD TSCM/Technical Service practitioners or DoD contractors who have successfully completed DoD-approved TSCM training shall conduct TSCM activities.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall:

5.1.1. Ensure that the Department of Defense has a viable TSCM policy and program.

5.1.2. Authorize appropriate DoD organizations to conduct TSCM, acquire and possess TSCM equipment, and have TSCM/Technical Service practitioners (Enclosure 4).

5.2. The Deputy Under Secretary of Defense (Counterintelligence and Security) (DUSD(CI&S)) shall:

5.2.1. Establish and sustain the DoD TSCM program.

5.2.2. Establish TSCM policy, establish standards, and approve waivers to this Instruction when necessary.

5.2.3. Serve as the advisor to the USD(I) regarding all TSCM matters.

5.3. The Director, CI, under the DUSD(CI&S), shall:

5.3.1. Provide oversight for the TSCM program.

5.3.2. Implement TSCM policy and standards.

5.3.3. Develop TSCM training and certification standards.

5.3.4. Participate in DoD and national-level forums concerning DoD TSCM.

5.3.5. Conduct reviews of TSCM research, development, test and evaluation (RDT&E) and training programs.

5.4. The Director, NSA/CSS, under the authority, direction, and control of the USD(I), shall:

5.4.1. Conduct laboratory analysis of materials and evidence collected from TSCM activity.

5.4.2. Disseminate technical penetration and technical hazard reports to the TSCM community through the Technical Security Portal (TSP) and/or the designated CI information system, as appropriate.

5.4.3. Provide technical and analytic support to reports and briefings on technical surveillance device finds.

5.4.4. Manage DoD TSCM RDT&E, training, and exercise support activities.

5.4.4.1. Operate the Interagency Training Center (ITC).

5.4.4.2. Develop and maintain currency of TSCM training courses.

5.4.4.3. Test and evaluate TSCM equipment.

5.4.5. Represent the Department of Defense, in collaboration with the Director, DoD CIFA, in TSCM RDT&E, training, and exercise management with foreign partners.

5.4.6. Conduct reviews and submit budgetary submissions for TSCM RDT&E and training matters funded in the Information Systems Security Program. Assist the Director, CI, DUSD(CI&S), in reviews of TSCM RDT&E and training programs.

5.4.7. Chair the DoD Technical Surveillance Integrated Management Group (TSIMG) on matters related to TSCM RDT&E, training, and exercises.

5.4.8. At least annually, chair a special TSIMG to discuss training curricula issues.

5.4.9. Implement, in coordination with the TSIMG, DoD TSCM certification and procedures.

5.4.10. Administer and maintain the TSP.

5.5. The Director, DoD CIFA, under the authority, direction, and control of the USD(I), shall:

5.5.1. Ensure the DoD TSCM program is coordinated, integrated, and synchronized with other CI missions and functions.

5.5.2. Manage the DoD TSCM Program.

5.5.3. Provide CI analytical support regarding technical surveillance threats to the Department of Defense.

5.5.4. Recommend policy changes through the Director, CI, to the DUSD(CI&S).

5.5.5. Serve as advisor to the DUSD(CI&S) regarding DoD TSCM matters.

5.5.6. Conduct TSCM program planning and ensure TSCM is adequately addressed in the DoD CI Strategy, consistent with DoD and national-level strategies and guidance.

5.5.7. Represent the Department of Defense with other U.S. Government and non-government agencies regarding the execution of the DoD TSCM program and policies.

5.5.8. Collaborate with the DoD TSCM community to review and make budget submissions.

5.5.9. Develop TSCM program resource and performance measurement standards.

5.5.10. Conduct reviews of the DoD Component TSCM programs.

5.5.11. Establish the TSIMG. See Enclosure 5.

5.5.12. Chair the TSIMG for all TSCM matters with the exception of TSCM RDT&E, training, and exercises (see paragraph 5.4.8.).

5.5.13. Ensure DoD TSCM reporting is entered into the designated CI information system and/or the TSP, as appropriate.

5.5.14. Through DUSD(CI&S), ensure USD(I) and other senior DoD officials are briefed regarding significant TSCM activity.

5.5.15. Notify the appropriate national-level authorities of technical penetrations.

5.6. The Heads of DoD Components shall:

5.6.1. Request TSCM services to ensure that sensitive working environments are free of technical surveillance devices, identify hazardous conditions that could facilitate technical

surveillance, identify conditions which are, or contribute to, technical security weaknesses, correct deficiencies, and employ countermeasures to defeat technical surveillance efforts.

5.6.2. Employ operations security regarding any proposed, planned, in progress, or completed TSCM service of a facility. This will prevent a compromise of TSCM tactics, techniques, and procedures.

5.7. The Heads of DoD Components with authorized TSCM organizations shall:

5.7.1. Manage the Component TSCM Program.

5.7.2. Submit to Director, DoD CIFA, as requested, TSCM program budgetary submissions and provide relevant information in support of reviews.

5.7.3. Participate in the TSIMG.

5.7.4. Submit TSCM technology requirements to the TSIMG.

5.7.5. Conduct TSCM and provide support to organizations without organic TSCM capability. See Enclosure 3.

5.7.6. Submit TSCM training requirements and training curricula requirements to the TSIMG.

5.7.7. Ensure that TSCM/Technical Service practitioners have successfully completed the ITC's TSCM Fundamentals Course.

5.7.8. Ensure that, at least annually, TSCM/Technical Services practitioners receive refresher or other specialized TSCM/Technical Services-related training.

5.7.9. Notify the DoD TSCM Program Manager of technical penetrations and other significant TSCM activity.

6. PROCEDURES

6.1. General

6.1.1. Component TSCM organizations shall prioritize TSCM requests.

6.1.2. TSCM requests shall only be approved for facilities, or categories of facilities, that the supporting TSCM organization has determined are probable and feasible targets for technical espionage or exploitation based on the value of the information processed in those facilities (facility technical threat analysis).

6.1.3. No facility will automatically receive a recurrent TSCM. Only authorized TSCM organizations determine whether or not a facility requires a recurrent TSCM. The facility technical threat analysis determines the frequency of recurring TSCM.

6.1.4. All foreign government requests for the release to or joint use of DoD TSCM equipment and techniques shall be approved through the Foreign Disclosure process according DoD Directive 5230.11 (Reference (e)) and DoD Directive C-5230.23 (Reference (f)). In Combatant, Joint, or Coalition Force environments, the TSCM organization shall concurrently notify the Combatant Command CI Staff Officer and the DoD TSCM Program Manager.

6.2. Requests

6.2.1. Request TSCM in accordance with procedures established by the supporting authorized TSCM organization.

6.2.2. Submit TSCM requests through secure communications. Secure voice requests are acceptable but must be followed, in a timely manner, by a written request. Secure voice requests shall not be made from within the facility for which the TSCM is being requested.

6.2.3. Conferences or sessions that require discussions of sensitive or classified information shall be held in cleared government or contractor facilities whose security is commensurate with the sensitivity of the information discussed according to the Assistant Secretary of Defense Memorandum (Reference (g)).

6.3. Senior Official Considerations. Senior officials, who must discuss sensitive or classified information while traveling, shall:

6.3.1. Use secure voice and data equipment.

6.3.2. Use technical countermeasure tools such as sound masking systems, sound isolation rooms, and radio frequency shielding tents/enclosures.

6.3.3. Use other technical protective techniques as recommended by the supporting authorized TSCM organization and/or cognizant Certified TEMPEST Technical Authority.

6.3.4. TSCM practitioners shall make all reasonable efforts to mitigate technical hazards and detect technical surveillance equipment in areas used by these officials.

6.4. Conduct of TSCM Services. TSCM services shall be conducted according to the Security Policy Board Procedural Guide (Reference (h)) and procedure 5 of DoD 5240.1-R (Reference (i)).

6.4.1. When CI considerations dictate variance from TSCM community technical guidelines, the on-site TSCM team leader will conduct the TSCM as is most appropriate for the situation.

6.4.2. Upon completion of a TSCM service where variances to the TSCM community technical guidelines were undertaken, an explanation of what necessitated the variance and the actions taken will be fully documented and forwarded to the Director, DoD CIFA.

6.4.3. The documented variances will be taken into consideration for revisions to DoD TSCM policy and/or TSCM community technical guides.

6.5. Reporting Requirements

6.5.1. No later than 10 duty days after completion of a TSCM service, a final report shall be forwarded to the requester. At a minimum, the report shall include the information prescribed in Enclosure 6, Information for TSCM Report.

6.5.2. All TSCM service reporting and feedback reports from the serviced agencies, in addition to any Component reporting requirements, will be entered into the designated CI information system and/or the TSP, as appropriate.

6.5.3. If a technical penetration is discovered, the servicing TSCM organization shall follow the guidance in the Security Policy Board Procedural Guides, Reference (j); immediately report the find, in coordination with the DoD TSCM Program Manager, to the USD(I); and employ appropriate sanitization procedures if special access programs are involved. Additionally, the responsible Combatant Command shall be informed of the discovery of any technical penetrations within their area of responsibility.

6.5.4. If a technical hazard is discovered, the servicing TSCM organization shall follow the guidance in the Security Policy Board Procedural Guides (Reference (k)). The hazard will be treated as a technical penetration until a thorough investigation indicates whether or not the condition has been exploited. The portion of the technical hazard report that identifies the finding shall be released to the customer and identified as a Technical Vulnerability. Technical hazard reports are for the CI/TSCM community and to provide guidance to technical security and/or TSCM RDT&E to develop countermeasures and are not intended for use outside of the community.

6.5.5. Upon receipt of a completed TSCM report with findings, the agency responsible for the facility has 30 calendar days to provide the servicing TSCM organization a report of corrective action taken, acceptance of risk, or a refutation of findings. Failure on the part of the receiving agency to provide this feedback will imply an acceptance of risk.

6.5.6. The reporting requirements in this Instruction are exempt from licensing according to paragraphs C4.4.2. and C4.4.8. of DoD 8910.1-M (Reference (l)).

6.6. Shipment of TSCM Equipment. Due to the extremely sensitive nature of the technology and capabilities associated with TSCM equipment, unaccompanied TSCM equipment and material shall be shipped through the Defense Courier Service, registered U.S. Mail, or other appropriate means.

6.7. In-Place Monitoring Systems. Commanders of highly sensitive projects or facilities who desire to augment their TSCM support may procure in-place monitor equipment. This is subject to pre-procurement coordination with the servicing authorized TSCM organization. The using DoD Component shall fund equipment purchase, installation, and operation. The DoD Component, working with the servicing authorized TSCM organization, shall ensure only trained, qualified personnel operate the in-place monitoring equipment. In-place monitoring equipment shall be operated according to DoD 5240.1-R, Reference (i).

6.8. Classification of TSCM Related Information. Information pertaining to the TSCM program shall be protected to preserve the integrity of the information and the program. Such information is classified according to DoD Instruction C-5240.8 (Reference (m)).

6.9. TSCM/Technical Service Practitioners and Training

6.9.1. Personnel. The nature of TSCM requires personnel who possess extensive knowledge in investigations, electronics, security evaluation, and construction. The minimum qualifications required for consideration for entry into the TSCM field are listed in Enclosure 7. In addition, the selection process shall include a personal interview and evaluation by a senior technical agent, as defined by the authorized TSCM organization.

6.9.2. Training. At a minimum, all TSCM/Technical Service practitioners shall successfully complete the ITC's TSCM Fundamentals Course. DoD Components shall ensure that their TSCM/Technical Service practitioners receive, at least annually, refresher or other specialized training to remain proficient and knowledgeable concerning unusual or new technical penetration and/or detection techniques.

6.9.2.1. TSIMG members will submit subject-matter training requirements to the NSA/CSS TSIMG representative and/or Director, ITC, for consideration in updating TSCM curricula.

6.9.2.2. The NSA/CSS representative to the TSIMG shall, at least annually, present current and proposed curricula for TSIMG review.

6.9.2.3. Annual refresher or other specialized training for TSCM/Technical Services practitioners may be received through a wide variety of methods to include in-house (at the unit level), in-residence, through mobile training team, through distance/distributed learning or any other method determined by the TSCM organization's and the individual TSCM/Technical Services practitioner's training needs.

6.9.2.3.1. When practicable, TSCM organizations shall use ITC presented or prepared TSCM annual refresher or other specialized training for their assigned TSCM/Technical Services practitioners.

6.9.2.3.2. TSCM organizations that receive non-ITC training shall submit a report to the TSIMG. The report shall identify the training institution or source and provide information on the content, objectives, materials, and value of the training. The TSIMG shall forward the report to the ITC. The ITC reviews the training and renders an opinion as to its

value. The ITC may incorporate the training into the ITC program. The ITC shall provide a listing of reviewed courses to the TSIMG.

6.10. TSCM Equipment Development and Procurement. The TSIMG determines the most effective equipment and techniques available to conduct TSCM (Enclosure 5). When making TSCM equipment procurement decisions, Component TSCM organizations shall consider interoperability with other Component TSCM organizations.

6.11. TSCM Equipment Disposition. The transfer of excess TSCM equipment between U.S. Government TSCM organizations is encouraged. All classified and sensitive but unclassified TSCM equipment declared obsolete and identified for disposal, when the equipment reveals countermeasures capabilities or limitations, shall be demilitarized according to DoD 4160.21-M-1 (Reference (n)). Remove identifying marks that associate the equipment with TSCM services.

6.12. Cross-Utilization of TSCM activities. Standardization of TSCM techniques, TSCM training, and TSCM equipment increases the potential for effective cross-utilization of TSCM among the DoD Components. Cross-utilization, where appropriate, is highly encouraged and shall be provided on a non-reimbursable basis.

6.13. TSCM with non-DoD US Agencies. DoD TCSM personnel may participate in TSCM with non-DoD U.S. agencies, upon concurrence of the appropriate TSCM organizational commander or his delegated representative. The TSCM organization shall report the conduct of TSCM with non-DoD U.S. agencies through the designated CI information system and/or the TSP, as appropriate.

7. EFFECTIVE DATE

This Instruction is effective immediately.

Stephen A. Cambone
Under Secretary of Defense for Intelligence

Enclosures - 7

E1. ENCLOSURE 1

REFERENCES, continued[1]

(e) DoD Directive 5230.11 “Disclosure of Classified Military Information to Foreign Governments and International Organizations,” June 16, 1992
(f) DoD Directive C-5230.23, “Intelligence Disclosure Policy,” November 18, 1983
(g) Assistant Secretary of Defense Memorandum, “Classified Information and Meetings and Conferences,” October 26, 2001
(h) Security Policy Board Issuance 1-99, Procedural Guide 1, "The Conduct of a Technical Surveillance Countermeasures Survey," March 24, 1999
(i) DoD 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,” December 1, 1982, authorized by DoD Directive 5240.1, April 25,1988
(j) Security Policy Board Issuance 1-99, Procedural Guide 2, "Requirements for Reporting and Testing of Technical Surveillance Penetrations," March 24, 1999
(k) Security Policy Board Issuance 1-99, Procedural Guide 3, "Requirements for Reporting and Testing of Technical Surveillance Hazards," March 24, 1999
(l) DoD 8910.1-M, "Procedures for Management of Information Requirements," June 30, 1998
(m) DoD Instruction C-5240.8, “Security Classification Guide for Information Concerning the DoD Counterintelligence Program," November 16, 2000
(n) DoD 4160.21-M-1, "Defense Demilitarization Manual," October 21, 1991

[1] References (f), (h), (j), (k), and (m) are available upon request from the Counterintelligence Directorate, DUSD(CI&S)/CI, Room 3C260, 5000 Defense Pentagon, Washington, DC 20301-5000

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Interagency Training Center (ITC). The NSA/CSS operated national center for TSCM training.

E2.1.2. Item of Security Interest. An unexploited condition that, by itself, is not a technical or physical vulnerability but can degrade or contributes to the degradation of the overall security posture of the area to the point where the condition could facilitate a technical or physical vulnerability.

E2.1.3. Physical Vulnerability. An unexploited condition occurring in the physical infrastructure of a facility that could facilitate the unauthorized removal of information bearing energy through either mechanical or electrical means.

E2.1.4. Technical Hazard. An unexploited condition wherein information-bearing energy might be intercepted and compromised.

E2.1.5. Technical Penetration. The use of technological means to conduct an intentional, unauthorized interception of information-bearing energy.

E2.1.6. Technical Security Portal (TSP). A DoD sponsored initiative focused on bringing together disparate data sources and applications that support threat analysts, TSCM evaluators, and subject matter experts into a single workspace to foster collaboration within the Technical Security Community.

E2.1.7. 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.

E2.1.8. Technical Threat Analysis. A continual process of compiling and examining all available information concerning potential technical surveillance activities by intelligence collection groups which could target personnel, information, operations, and resources.

E2.1.9. Technical Vulnerability. See Technical Hazard, or an unexploited electromechanical condition wherein information-bearing energy might be intercepted but does not contain actionable information.

E3. ENCLOSURE 3

LEAD AGENCIES FOR TSCM ACTIVITIES IN DEFENSE ORGANIZATIONS WITHOUT ORGANIC TSCM ASSETS[2]

Defense Components	Lead Agency
Missile Defense Agency	Air Force Office of Special Investigations
Defense Advanced Research Projects Agency	Naval Criminal Investigative Service
Defense Commissary Agency	U.S. Army Intelligence and Security Command
Defense Contract Audit Agency	U.S. Army Intelligence and Security Command
Defense Contract Management Agency	U.S. Army Intelligence and Security Command
Defense Criminal Investigative Service	Air Force Office of Special Investigations
Defense Finance and Accounting Service	Naval Criminal Investigative Service
Defense Information Systems Agency	Naval Criminal Investigative Service
Defense Legal Services Agency	Air Force Office of Special Investigations
Defense Logistics Agency	U.S. Army Intelligence and Security Command
Defense Security Cooperation Agency	Air Force Office of Special Investigations
Office of the Secretary of Defense	Pentagon Force Protection Agency
National Geospatial-Intelligence Agency	U.S. Army Intelligence and Security Command
United States Central Command	Air Force Office of Special Investigations
United States European Command	U.S. Army Intelligence and Security Command
United States Forces Korea	U.S. Army Intelligence and Security Command
United States Joint Forces Command	Naval Criminal Investigative Service
United States Northern Command	Air Force Office of Special Investigations
United States Pacific Command	Naval Criminal Investigative Service
United States Southern Command	U.S. Army Intelligence and Security Command
Unites States Special Operations Command	Air Force Office of Special Investigations
United States Strategic Command	Air Force Office of Special Investigations
United States Transportation Command	Air Force Office of Special Investigations

[2] Any other DoD TSCM requirements will be specified by the DoD TSCM Program Manager in coordination with the TSIMG. The DoD TSCM Program manager shall coordinate TSCM support for Defense Security Service.

E4. ENCLOSURE 4

LIST OF AUTHORIZED ORGANIZATIONS

E4.1. The following are the authorized DoD TSCM organizations:

U.S. Army Intelligence and Security Command
650th Military Intelligence Group
Naval Criminal Investigative Service
Marine Corps Intelligence
Air Force Office of Special Investigations
National Security Agency/Central Security Service
Defense Intelligence Agency
DoD Counterintelligence Field Activity
Defense Threat Reduction Agency
The Joint Staff
Pentagon Force Protection Agency
White House Communications Agency
National Reconnaissance Office

E4.2. Other DoD Components as authorized by USD(I) memoranda.

E5. ENCLOSURE 5

DoD TSIMG CHARTER

E5.1. Purpose

E5.1.1. The TSIMG facilitates information sharing among DoD TSCM professionals.

E5.1.2. The TSIMG collaborates with its membership to identify DoD TSCM program related problems and then determines courses of action to rectify those problems.

E5.2. Organization. The TSIMG is composed of representatives of the DoD TSCM organizations, the DoD TSCM Program Management Office, and the NSA/CSS TSCM RDT&E and TSCM training managers.

E5.3. Roles and Responsibilities

E5.3.1. The DoD CIFA representative will serve as the TSIMG Chair. The NSA/CSS representative will chair TSIMG meetings, or portions thereof, during which TSCM RDT&E, TSCM exercise(s), or TSCM training issues are discussed.

E5.3.2. If the primary TSIMG representative is unable to attend a meeting, a suitable alternate from that TSCM organization shall attend. The alternate assumes the duties and responsibilities of the primary member.

E5.3.3. The TSIMG recommends TSCM policy changes.

E5.4. Process

E5.4.1. At a minimum, the TSIMG will meet semiannually.

E5.4.2. The TSIMG will conduct annual reviews of TSCM training (to include course curricula), DoD-related TSCM exercises, and TSCM RDT&E**.**

E6. ENCLOSURE 6

INFORMATION FOR TSCM REPORT

E6.1. Reports shall be prepared and distributed to requestors, monitoring agencies (a monitoring agency is one that has security cognizance over the facility receiving the TSCM), and the TSCM organizations' responsible representatives. As a minimum, reports shall contain the following information:

E6.1.1. Unit identification, address (if applicable), and geographic location (also account number if National Communications Security Instruction Survey).

E6.1.2. Requestor information.

E6.1.3. Date(s) accomplished.

E6.1.4. Brief description of support provided, for example, a complete or partial TSCM service, an in-place monitor, or other TSCM activity.

E6.1.5. Findings. Report in detail discovered security vulnerabilities or items of security interest.

E6.1.6. Recommendations. Include recommendations on how to eliminate or substantially mitigate each item of security interest or vulnerability. Carefully develop recommendations to ensure they will effectively correct the deficiency and that they are cost effective.

E6.1.7. Name(s) of the local person(s) briefed on the results of the TSCM service.

E6.2. Report specific equipment and new or unusual techniques or methods used. Report through the designated CI information system and/or the TSP, as appropriate.

E7. ENCLOSURE 7

QUALIFICATION FOR ENTRY INTO TSCM FIELD

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

E7.1.1. Education. At a minimum, the candidate must have a high school diploma or equivalent and must have completed a course in electronics fundamentals.

E7.1.2. 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.

E7.1.3. Clearance. TOP SECRET, eligible for access to Sensitive Compartmented Information.

E7.1.4. Grade. E-5 or higher, or a civilian grade as determined by the authorized TSCM organization.

E7.1.5. Age. Twenty-one years or older.

E7.1.6. Physical. The TSCM applicant shall meet physical standards set forth by each DoD TSCM organization. The minimum DoD requirements are:

E7.1.6.1. 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.

E7.1.6.2. 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.

E7.1.6.3. Color perception test results, employing the pseudo-isochromatic plates for testing color perception, not to exceed four incorrect identifications out of fourteen test plates.

E7.1.6.4. Free from any physical problems which materially hinder manual dexterity. Applicant must have normal range of motion in all extremities.

E7.1.6.5. 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:

E7.1.6.5.1. Ability to lift forty pounds overhead, using both arms.

E7.1.6.5.2. Ability to carry forty pounds in a manner similar to carrying a suitcase.

E7.1.6.5.3. Ability to climb a six-foot ladder**.**

E7.1.6.5.4. Ability to crawl beneath a three-foot barrier**.**