Department of Defense
INSTRUCTION

NUMBER 5240.05
April 3, 2014

USD(I)

SUBJECT: Technical Surveillance Countermeasures (TSCM)

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), this instruction:

a. Reissues DoD Instruction (DoDI) 5240.05 (Reference (b)) to establish policy and assign responsibilities for TSCM.

b. Implements procedures for DoD TSCM in accordance with DoDD O-5240.02 (Reference (c)).

c. Refines organizational relationships in accordance with DoDI 5240.10 (Reference (d)).

d. Defines the role of TSCM as one of the counterintelligence (CI) functional services in accordance with DoDI 5240.16 (Reference (e)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. It is DoD policy that:

a. TSCM will be conducted to detect, neutralize, and exploit technical surveillance and associated devices, technologies, and hazards that facilitate the unauthorized or inadvertent access to or removal of DoD information in accordance with Reference (c).

b. Only DoD personnel who have successfully completed approved TSCM training will conduct TSCM.

c. Only organizations authorized in Enclosure 4 and subsequently approved to conduct TSCM will acquire, possess, or employ equipment and personnel for the purpose of detecting technical surveillance and associated devices, technologies, and hazards.

d. As designated in Enclosure 5, organizations will provide TSCM support to the DoD Components that lack an organic TSCM capability.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Unlimited**. This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction:

a. Is effective April 3, 2014.

b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoD Instruction 5025.01 (Reference (f)).

c. Will expire effective April 3, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (f).

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. Procedures
4. Organizations Authorized to Conduct TSCM
5. TSCM Support to DoD Components Without A TSCM Capability
6. DoD TSCM IMG Charter

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(b) DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM) Program," February 22, 2006 (hereby cancelled)
(c) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007, as amended
(d) DoD Instruction 5240.10, "Counterintelligence (CI) in the Combatant Commands and Other DOD Components," October 5, 2011, as amended
(e) DoD Instruction 5240.16, "Counterintelligence Functional Services (CIFS)," August 27, 2012, as amended
(f) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended
(g) DoD Instruction 3305.11, "DoD Counterintelligence (CI) Training," March 19, 2007, as amended
(h) DoD Instruction 3305.12, "Intelligence and Counterintelligence (I&CI) Training of Non-U.S. Persons," October 25, 2007, as amended
(i) DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004
(j) DoD S-5240.05-M-1, "The Conduct of Technical Surveillance Countermeasures (U)," April 30, 2007
(k) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982
(l) DoD Instruction C-5240.08, "Counterintelligence (CI) Security Classification Guide (U)," November 28, 2011
(m) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(n) Director of Central Intelligence Directive 5/1P, "Espionage and Counterintelligence Activities Abroad," December 19, 1984

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I):

a. Serves as the TSCM advisor to the Secretary of Defense .

b. Authorizes DoD organizations to conduct TSCM.

c. Delegates authority to the Secretaries of the Military Departments in accordance with Enclosure 3 to authorize the creation of TSCM programs within their respective Departments.

2. DEPUTY DIRECTOR FOR INTELLIGENCE (INTELLIGENCE AND SECURITY) (DDI(I&S)). Under the authority, direction, and control of the USD(I), the DDI(I&S):

a. Develops and recommends TSCM policy to the USD(I).

b. Provides TSCM policy oversight.

c. Provides direction for exploiting a discovered technical surveillance.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in sections 5 and 6 of this enclosure, the Director, DIA, oversees TSCM and:

a. Appoints the TSCM functional manager.

b. Notifies the USD(I), DDI(I&S), and other senior DoD officials regarding TSCM technical surveillances, trends, and issues.

c. Represents the DoD TSCM community at national TSCM forums, except as noted below.

d. In coordination with the TSCM organizations in Enclosure 4, develops and establishes TSCM resource and performance measurement standards.

e. Conducts reviews of the TSCM organizations at least biennially.

f. Chairs the TSCM Integrated Management Group (IMG).

g. Ensures DoD TSCM reporting is documented in the USD(I)-approved CI information system.

h. Recommends TSCM changes in DoD policy, procedures, standards, doctrine, and planning documents.

i. Coordinates with the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) concerning funding for TSCM research, development, test, and evaluation (RDT&E), exercises, and training.

j. Provides and coordinates CI analytical support regarding foreign intelligence entity (FIE) technical surveillance threats.

k. Recommends the assignment of lead responsibilities for on-site coordination in a joint operating environment.

l. In coordination with the TSCM IMG and the Interagency Training Center (ITC), establishes TSCM training standards and practices.

m. Maintains, by fiscal year, TSCM metrics on:

(1) The number of TSCM reports generated.

(2) The number and description of technical surveillances and hazardous conditions identified during TSCM.

n. Publishes procedural guides or standards for use by the DoD TSCM community.

o. Notifies the appropriate DoD and national-level authorities of technical surveillances and hazardous conditions.

p. Provides an annual review to the DDI(I&S) of DoD TSCM capabilities and activities.

4. DIRNSA/CHCSS. Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in sections 5 and 6 of this enclosure, the DIRNSA/CHCSS:

a. Coordinates, conducts, and manages DoD TSCM RDT&E, training, and exercise support.

b. Provides the customer, supporting TSCM organization program manager, and the Director, DIA, with preliminary analysis of TSCM materials and evidence within 10 business days of receipt and a final report within 60 business days of receipt, as resources and priorities permit or upon mutual agreement with the customer.

c. Represents DoD at national-level TSCM forums with regard to TSCM RDT&E, training, and exercise activities.

d. Represents DoD, in coordination with the Director, DIA, in TSCM RDT&E, training, and exercise management with foreign partners.

e. Coordinates with the Director, DIA, regarding the release of TSCM training materials to foreign governments.

f. Operates and maintains the ITC and the Interagency Test and Evaluation Laboratory (ITEL).

g. Notifies the Director, DIA, of ITC and ITEL activities supporting TSCM.

h. Conducts reviews and submits budget requirements for TSCM RDT&E and training matters funded in the Information Systems Security Program.

i. Executes TSCM training standards and recommends the TSCM practitioners certification process in coordination with the TSCM IMG and the DoD CI and Human Intelligence (HUMINT) Training Council in accordance with DoDI 3305.11 (Reference (g)) and DoDI 3305.12 (Reference (h)).

j. Operates a technical security analysis capability.

k. Distributes technical surveillance device and hazard reports to the DoD Components through the USD(I)-approved CI information system, as appropriate.

l. Provides training products and briefings to increase awareness of the technical threat.

m. Coordinates with the Director, DIA, concerning funding for TSCM RDT&E and other enterprise wide TSCM capability.

n. Publishes training guides or standards for use by the DoD TSCM community.

o. Provides training through the ITC for TSCM practitioners to meet the minimum training requirements for access to DoD networks in accordance with DoDD 8570.01 (Reference (i)).

5. DoD COMPONENT HEADS. The DoD Component heads:

a. Request TSCM support to ensure sensitive and classified working environments are free of technical surveillances and hazards.

b. Respond to TSCM reports within 90 business days to address corrective actions, acceptance of risk, or refutation of findings.

c. Coordinate with the supporting TSCM organization in conducting a damage assessment when technical surveillance is discovered and submit the assessment to the Director, DIA.

d. Employ operations security with any proposed, planned, in-progress, or completed TSCM.

e. Permit the access of TSCM practitioners, technicians, and equipment into facilities where technical surveillance is discover or TSCM is requested or required.

f. In coordination with the supporting TSCM organization, establish procedures to notify the appropriate authorities if a suspected technical surveillance is discovered in accordance with section 3 of Enclosure 3.

g. Permit access by TSCM practitioners and technicians, and equipment onto information systems and networks.

(1) Confirm that the TSCM practitioners meet the minimum training requirements for unsupervised access to DoD networks in accordance with Reference (i).

(2) Permit the properly trained TSCM practitioner full administrator privileges to the systems involved in the TSCM.

h. Request TSCM program authorization from the Secretary of the Military Department to which the organization belongs or the USD(I), as appropriate.

i. Ensure any TSCM-unique equipment remains in the custody of the TSCM organization.

6. DoD COMPONENT HEADS WITH TSCM ORGANIZATIONS. In addition to the responsibilities in section 5 of this enclosure, the DoD Component heads with TSCM organizations:

a. Appoint a TSCM program manager.

b. Establish written TSCM procedures and integrate TSCM with CI missions and functions.

c. When requested, provide the Director, DIA, with TSCM budgetary submissions and relevant information in support of TSCM reviews.

d. Support designated DoD Components in accordance with Enclosure 5.

e. Ensure TSCM practitioners are trained and certified in accordance with Enclosure 3.

f. May develop the use of TSCM technicians in accordance with Enclosure 3 to assist TSCM practitioners in the execution of the Component TSCM requirements.

g. Immediately notify the DoD TSCM functional manager of the discovery of a technical surveillance.

h. Ensure TSCM reporting is documented in the USD(I)-approved CI information system.

i. Notify the supporting Military Department CI organization (MDCO) of all discoveries of suspected surveillances and hazardous conditions.

j. Coordinate with the DIRNSA/CHCSS for technical and analytic support to reports and briefings on devices found by TSCM practitioners, as appropriate.

k. Provide a representative to the TSCM IMG.

l. Annually, provide the TSCM IMG and ITC with TSCM training requirements.

m. Ensure TSCM practitioners meet the minimum training requirements for access to DoD networks in accordance with Reference (i).

n. Notify the USD(I) and Director, DIA, when opening or closing a TSCM program.

7. SECRETARIES OF THE MILITARY DEPARTMENTS. In accordance with Enclosure 3 and in addition to the responsibilities in section 5 and 6 of this enclosure, the Secretaries of the Military Departments:

a. May authorize TSCM programs within their respective Departments and possess equipment for TSCM.

b. Will notify the USD(I) and Director, DIA, when new TSCM programs are authorized and when existing programs are closed within their respective Departments.

ENCLOSURE 3

PROCEDURES

1. GENERAL

a. TSCM activities are conducted in accordance with DoD S-5240.05-M-1 (Reference (j)) and DoD 5240.1-R (Reference (k)).

b. The two levels of DoD trained TSCM personnel who may either conduct or assist in the conduct of TSCM are TSCM practitioners and TSCM technicians.

c. TSCM practitioners will:

(1) Complete the ITC Fundamentals course.

(2) Complete at least 40 hours of discipline-specific development or refresher training every fiscal year. The development or refresher training may consist of classroom, video, on-line, or commercially-available training or exercises.

(3) Have a Top Secret security clearance with sensitive compartmented information (SCI) access.

(4) Be certified by their DoD Component head to conduct TSCM with at least the training requirements of paragraph 1c.

(5) In a reasonable amount of time, respond to the discovery of a suspected technical surveillance device.

d. TSCM technicians will:

(1) Be associated with an authorized TSCM program.

(2) Conduct TSCM under the oversight of a TSCM practitioner.

(3) At a minimum, have at least a Secret security clearance. A higher level clearance is required for certain missions.

2. REQUESTS AND REPORTING REQUIREMENTS

a. Customers request TSCM support:

(1) In accordance with the supporting TSCM organizational procedures.

(2) Via secure communications from outside the area or facilities that will receive the TSCM support. Verbal requests must be followed with written documentation within 24 hours.

b. TSCM program managers:

(1) Prioritize support requests considering TSCM requirements and threat assessments.

(2) Recommend the use of a facility technical threat analysis to determine if a TSCM is warranted. Facilities may not automatically receive a recurrent TSCM.

(3) Upon receipt of a TSCM request, notify the customer of approval or of disapproval with written justification. A timeline of when TSCM will be provided may be given to the customer at the DoD Component TSCM program manager's discretion, based on the TSCM organization's policies, individual mission circumstances, and operational security requirements. If additional information would justify an approval, customers may request reevaluation.

(4) 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.

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

(6) Record TSCM reporting and feedback into the USD(I)-approved CI information system.

(7) Develop the capability, resources permitting, of CI-focused TSCM targeting using a risk-based approach with the goal of identifying and exploiting technical collection efforts targeting DoD interests.

3. DISCOVERY OF SUSPECTED TECHNICAL SURVEILLANCE

a. Upon discovery of a suspected technical surveillance, immediately:

(1) Secure the area to prevent unauthorized access or removal of any device.

(2) Maintain a normal working environment to prevent alerting the FIE of the discovery of suspected technical surveillance.

(3) Classify information regarding the discovery of a suspected technical surveillance in accordance with DoDI C-5240.08 (Reference (l)).

(4) Conduct communications regarding suspected technical surveillance outside the area containing the surveillance device and via secure means.

(5) Notify the responsible security manager.

(6) Notify the supporting TSCM organization in accordance with Enclosure 4 via secure communications. If direct reporting is not feasible, report the discovery through the security manager.

b. The security manager or responsible official will:

(1) Notify the supporting MDCO or supporting DoD Component TSCM organization.

(2) Prevent removal or tampering with a suspected technical surveillance device unless a potential exists for physical danger to personnel or property.

(3) Ensure TSCM practitioners and technicians can access the area.

(4) Limit knowledge of the discovery to only those with an immediate need to know.

(5) Notify the appropriate Military Department, agency, or command security officer of the discovery.

(6) Document all personnel with knowledge of the discovery. Include full name, grade, position, and date each individual was briefed. Provide this list to the responding TSCM team.

c. Supporting TSCM team personnel will:

(1) Notify the DIRNSA/CHCSS or designee of any known or suspected compromise involving cryptographic systems.

(2) Notify the DoD TSCM functional manager who will notify the DDI(I&S) and the National TSCM Program Office.

d. The supporting MDCO will coordinate with the TSCM organization that discovered the technical surveillance, the organizational commander of the location of the discovery, and the DDI(I&S) to determine the appropriateness of exploitation of the surveillance.

4. IN-PLACE MONITORING SYSTEMS. Commanders or directors of sensitive projects or facilities who desire to augment their TSCM support may install in-place monitoring equipment under the following conditions. The commanders or directors will:

a. Coordinate with the supporting TSCM program manager and legal advisor prior to obtaining any equipment.

b. Coordinate with the supporting TSCM program manager and the Director, DIA, to develop an operational plan.

c. Fund developmental and coordination costs, equipment purchases, installation, life-cycle costs, training, and operation for in-place monitoring, including an alert response capability and plans.

d. Coordinate with the supporting TSCM program manager to ensure only trained and qualified personnel operate the in-place monitoring equipment.

e. Ensure the operational plan includes reporting procedures for discovery of actual or suspected technical surveillances and hazards in accordance with this instruction and supporting TSCM organizational requirements.

f. Dispose of in-place monitoring systems in accordance with section 5.

5. TSCM EQUIPMENT, PROCUREMENT, AND DISPOSITION. Before disposing of excess TSCM equipment, DoD Component TSCM organizations will:

a. Offer the equipment to other DoD Component TSCM organizations and then to national TSCM organizations, in accordance with appropriate DoD policy.

b. Demilitarize TSCM equipment that reveals countermeasures capabilities or limitations and is declared obsolete and identified for disposal in accordance with DoD Component procedures.

c. Remove identifying marks that associate the equipment with TSCM.

6. SPECIAL CIRCUMSTANCES. Personnel who must process sensitive or classified information while outside of secure or controlled facilities will:

a. Consult with the supporting TSCM program manager to identify the type and level of required TSCM support.

b. Use secure voice and data equipment to transmit sensitive and classified information.

c. Employ countermeasures as recommended by the supporting TSCM organization based on specific threat information.

d. Conduct TSCM at classified meetings and conferences in accordance with Volume 3 of DoD Manual 5200.01 (Reference (m)).

7. INVOLVEMENT WITH NON-DoD AGENCIES

a. TSCM practitioners may conduct TSCM with non-DoD federal agencies after approval by the appropriate authority.

(1) The TSCM program manager will coordinate with the appropriate legal counsel and notify the Director, DIA, or designee.

(2) The TSCM program manager will report the conduct of TSCM activities with non-DoD agencies through the USD(I)-approved CI information system.

b. Upon receipt of foreign military requests for the release or joint use of TSCM equipment and techniques, TSCM program managers:

(1) Must coordinate with the foreign disclosure officer and, as appropriate, the international engagement office in accordance with Component procedures.

(2) In Combatant Command, joint, or coalition force environments, concurrently coordinate with the command CI coordinating authority and the Director, DIA.

c. TSCM conducted outside of the continental United States in non-U.S. government controlled areas will be coordinated in accordance with Director of Central Intelligence Directive 5/1P (Reference (n)) or its successor.

ENCLOSURE 4

ORGANIZATIONS AUTHORIZED TO CONDUCT TSCM

1. Organizations currently authorized to conduct the full range of TSCM, including acquiring, possessing, and using equipment designed for the conduct of TSCM, are:

a. Department of the Army

(1) U.S. Army Intelligence and Security Command

(2) 650th Military Intelligence Group

(3) United States Army Special Operations Command

b. Department of the Navy

(1) Naval Criminal Investigative Service

(2) Marine Corps Intelligence

c. Department of the Air Force Air Force Office of Special Investigations

d. The Joint Staff

e. The Joint Special Operations Command

f. National Security Agency/Central Security Service

g. Defense Advanced Research Projects Agency

h. DIA

i. Defense Threat Reduction Agency

j. Missile Defense Agency

k. National Geospatial-Intelligence Agency

l. National Reconnaissance Office

m. Pentagon Force Protection Agency

n. White House Communications Agency

o. United States Special Operations Command (Central)

2. Other DoD Components may be given authority to conduct the full range of TSCM, as authorized by USD(I) memorandums or under the authority referenced in section 3 of Enclosure 2.

ENCLOSURE 5

TSCM SUPPORT TO DoD COMPONENTS WITHOUT A TSCM CAPABILITY

The tables in this enclosure establish the TSCM relationship between the supporting TSCM organizations from Enclosure 4 and the supported organizations. These relationships are for the use of TSCM only, as established in this instruction, and are separate from the relationships between the MDCOs and supported headquarters established in Reference (d).

Table 1. Supporting TSCM Organizations to the Defense Agency Headquarters and the OSD Staff

Supporting TSCM Organizations	Defense Agency Headquarters and the OSD Staff
U. S. Army Intelligence and Security Command	Defense Commissary Agency Defense Contract Management Agency Defense Contract Audit Agency Defense Logistics Agency Defense Security Service Secretary of Defense Travel Support
Naval Criminal Investigative Service	Defense Finance and Accounting Service
Air Force Office of Special Investigations	Defense Information Systems Agency Office of the Inspector General of the Department of Defense Defense Security Cooperation Agency
Pentagon Force Protection Agency	All OSD Staff Offices other than those listed in this enclosure assigned to other TSCM organizations. These offices include: Washington Headquarters Services Offices of the Under Secretaries Offices of the Assistant Secretaries Defense Media Activity Office of Economic Adjustment

Table 2. Supporting TSCM Organizations to the Combatant Command Headquarters

Supporting TSCM Organizations	Combatant Command Headquarters
U. S. Army Intelligence and Security Command	United States Africa Command United States European Command United States Southern Command United States Forces Korea
Naval Criminal Investigative Service	United States Pacific Command
Air Force Office of Special Investigations	United States Northern Command United States Strategic Command United States Transportation Command United States Special Operations Command United States Central Command
National Security Agency	United States Cyber Command

Table 3. Supporting TSCM Organizations to the DoD Field Activity Headquarters

Supporting TSCM Organizations	DoD Field Activity Headquarters
U. S. Army Intelligence and Security Command	Defense Technical Information Center
Naval Criminal Investigative Service	DoD Test Resource Management Center DoD Education Activity TRICARE Management Activity DoD Human Resources Activity
Air Force Office of Special Investigations	Defense Prisoner of War/Missing Persons Office Defense Technology Security Administration

ENCLOSURE 6

DoD TSCM IMG CHARTER

1. PURPOSE. The TSCM IMG, the principal forum for information sharing among TSCM practitioners, collaborates with its membership to identify TSCM-related issues and helps propose solutions to those issues.

2. MEMBERSHIP

a. The Director, DIA, appoints the chair.

b. The TSCM IMG is composed of representatives of the TSCM organizations, the DIRNSA/CHCSS RDT&E, and the ITC.

c. The chair may allow non-voting observers, including other full-time or permanent part-time federal employees.

3. MEETINGS

a. The TSCM IMG meets at least quarterly.

b. The chair publishes the meeting agenda at least 1 week prior to any meeting based on input provided by the members. When agenda items pertain to RDT&E, training, or exercise activities, the National Security Agency/Central Security Service representative will chair that portion of the meeting.

4. ACTIVITIES. The TSCM IMG:

a. Shares information among DoD TSCM practitioners.

b. Identifies DoD-wide TSCM problems and works collectively to provide potential solutions.

c. Provides input and feedback to DDI(I&S) regarding TSCM policy.

d. Recommends to the Director, DIA, resource and performance measurement standards.

e. Recommends applicant entrance training requirements, as well as TSCM training topics to the Director, ITC.

f. Assists the DIRNSA/CHCSS in developing TSCM practitioner certification standards.

g. At least annually, conducts a dedicated TSCM IMG, chaired by the representative of the DIRNSA/CHCSS, to review and discuss TSCM training (including course curriculum), RDT&E, and exercises.

h. Identifies core TSCM equipment.

i. Establishes, with the consent of the TSCM IMG membership, minimum standards for personnel entering the TSCM field.

j. Develops community-level proactive TSCM methodologies to combat the foreign technical surveillance threat.

k. Serves as the gateway for TSCM issues from the Components to the DoD counterterrorism and HUMINT governance process.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CI	counterintelligence
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoDD	DoD Directive
DoDI	DoD Instruction
DDI(I&S)	Deputy Director for Intelligence (Intelligence & Security)
FIE	foreign intelligence entity
HUMINT	human intelligence
ITC	Interagency Training Center
ITEL	Interagency Test and Evaluation Laboratory
MDCO	Military Department counterintelligence organization
RDT&E	research, development, test, and evaluation
TSCM	technical surveillance countermeasures
TSCM IMG	technical surveillance countermeasures Integrated Management Group
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this instruction.

hazard or hazardous condition. A condition, either technical or physical, that could permit the exfiltration and exploitation of information.

proactive TSCM. CI-focused TSCM targeting using a risk-based approach with the goal of identifying and exploiting technical collection efforts targeting DoD interests.

surveillance device. A piece of equipment or mechanism used to gain unauthorized access to and removal of information

technical surveillance. The use of optical, audio, or electronic monitoring devices or systems to surreptitiously collect information.

technical threat analysis. A continual process of compiling and examining information on technical surveillance activities against personnel, information, operations, and resources.

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

TSCM practitioner. An individual trained and certified to conduct all TSCM activities within DoD.

TSCM technician. An individual trained to perform limited TSCM activities under the oversight of a TSCM practitioner.

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.