BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 71-101, VOLUME 3

21 MAY 2019

Special Investigations

THE AIR FORCE TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing web site at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/IGX

Certified by: SAF/IG
(Lt Col Courtney R. Holland)

Supersedes: AFI 71-101 V3, 13 May 2015

Pages: 27

This publication implements Air Force Policy Directive (AFPD) 71-1, *Criminal Investigations and Counterintelligence*; and Intelligence Community Directive (ICD) 702, *Technical Surveillance Countermeasures*. It applies to the Air Force, Air Force Reserve, the Air National Guard (ANG) and the Civil Air Patrol (CAP), both military and civilian, performing an Air Force assigned mission and, as it pertains to submitting requests, Air Force Office of Special Investigations (AFOSI)-supported Defense Components listed in DoDI 5240.05, *Technical Surveillance Countermeasures (TSCM)*, Enclosure 3. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestors commander for non-tiered compliance items. This AFI may be supplemented at any level, but all supplements will be routed to the Office of Primary Responsibility (OPR) for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through appropriate chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include updates to the roles and responsibilities of the AFOSI Investigations Collections Operations Nexus (ICON) Center, adds instructions for the discovery of malicious network entities, and adds tiered waiver authorities for unit level compliance items.

Chapter 1

OVERVIEW

1.1. Technical Surveillance Countermeasures (TSCM). TSCM includes techniques and measures to detect, neutralize, and/or exploit a wide variety of hostile and foreign penetration technologies used to obtain unauthorized access to classified and sensitive information. DoDI 5240.05, designates the AFOSI as the only Air Force (AF) organization authorized to perform TSCM activities.

1.1.1. ICD 702 establishes Director of National Intelligence (DNI) policy and assigns responsibilities for oversight of the Intelligence Community (IC) TSCM programs.

1.1.2. *The National Technical Surveillance Countermeasures Strategy of the United States of America* sets mission and enterprise objectives for IC TSCM programs.

1.1.3. Legal authority to conduct TSCM is outlined in DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities.*

1.1.4. DoDI 5240.05 defines the role of TSCM as a counterintelligence (CI) functional service. This issuance applies to the Office of the Secretary of Defense, military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint 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 within the DoD.

1.1.5. DoDM S-5240.05, *The Conduct of Technical Surveillance Countermeasures (TSCM)*, establishes guidelines and procedures for the conduct of TSCM activities in the DoD. Military Service Memorandums of Understanding (MOUs) detail agreements between the Department of the Army G2X, Naval Criminal Investigative Service, U.S. Marine Corps Director of Intelligence and AFOSI on the provision of cross-service TSCM support to each other as well as providing TSCM support during conflicts, contingencies, or security and stability operations.

1.2. Philosophy of TSCM Activities. Technical surveillance may be the last information collection method of choice to U.S. adversaries. Turning to technical surveillance may be the result of the failure of other intelligence collection attempts (e.g., cyber, human intelligence, signals intelligence, etc.), there is no other way to obtain the desired information, or as a demonstration of will or capability. AF organizations employ comprehensive mitigation efforts including counterintelligence, security, and information assurance procedures, to counter technical security threats.

1.2.1. Adversaries include Foreign Intelligence Entities (FIE), organized crime, drug traffickers, terrorists, persons engaged in industrial espionage, dissident groups, and others with interest in U.S. information.

1.2.2. Our adversaries seek information to support bargaining positions (diplomatic), asset information (intelligence), personal data (counterintelligence), battle plans (national defense), economic data (diplomatic/criminal), or law enforcement data (criminal).

1.2.3. Technical surveillance usually takes the form of devices or software installed for the specific purpose of audio, visual, or data collection of information from a sensitive area. Direct technical penetration, exploitation of a technical vulnerability, or physical security weakness could obtain this information. Devices employed may range from simple wired microphones to sophisticated software or remote controlled devices and may use existing infrastructures such as networks, telephone, power lines, etc., to facilitate the surveillance.

1.3. Scope of TSCM Activities.

1.3.1. AFOSI identifies and focuses TSCM efforts on likely targets of FIE or other adversaries intent on collecting sensitive or classified U.S. information through technical means.

1.3.2. Anywhere there is classified or sensitive information discussion or processing, one can perform TSCM activities. This includes government and commercial facilities, aircraft, boats, vehicles, and hotel rooms, as appropriate. TSCM activities use techniques and specialized equipment to deter, detect, neutralize, and/or exploit technical penetration technologies used to obtain unauthorized access to classified and sensitive information. TSCM also includes customer education to help defend against technical surveillance exploitation.

1.3.3. TSCM activities are used to detect and/or prevent technical penetrations. Penetrations are the intentional, unauthorized interception of information-bearing energy such as establishment of a clandestine transmission path to provide egress of a technical surveillance product.

1.3.4. AFOSI coordinates with the DNI in accordance with ICD 304, *Human Intelligence*, and ICD 310, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States*, for TSCM activities conducted outside the U.S. off of DoD or U.S.-controlled installations.

1.4. Limitations of TSCM Activity.

1.4.1. TSCM activities are not a substitute for proper security practices. Physical, personnel and industrial security practices are the most effective impediments to a technical penetration. The following security practices affect the long-term validity of a TSCM:

1.4.1.1. Maintaining a continuous and verifiable access control program.

1.4.1.2. Controlling the acquisition, shipment, storage, and maintenance of equipment and furnishings.

1.4.1.3. Implementing a strict oversight and security program during construction and renovation.

1.4.1.4. Using cleared and qualified personnel with controlled equipment to design, install, and maintain intrusion detection and access control systems.

1.4.1.5. Using cleared and qualified personnel for the design and maintenance of information systems.

1.4.2. TSCM is not a compliance-oriented activity. However, it is an acceptance of risk by customers who fail to address any security issues identified during a TSCM.

1.4.2.1. A requestor is given reasonable assurance the surveyed area is free of active technical surveillance devices upon TSCM activity completion. The requestor also learns the overall security posture of the facility, to include all security vulnerabilities discovered within the area and receives a suggested course of action to correct them. However, the requestor should know it is impossible to provide an absolute guarantee there are no devices in a surveyed area.

1.4.2.2. The TSCM activity does not in itself eliminate existing security vulnerabilities, nor ensure the technical security status of the area cannot subsequently change. Uncontrolled access by unauthorized or uncleared persons; the introduction of new furnishings, equipment, or construction; or alterations within the area could result in the placement of a clandestine device and nullify any existing technical security vulnerabilities. Keep high standards of physical, personnel and industrial security to maintain the validity of the survey.

1.4.2.3. TSCM activities are usually a one-time evaluation after a validated threat assessment identifies the facility may be a likely target of technical surveillance. Any assurance of protection remains in effect until there is a physical (construction in facility), personnel, or industrial security (uncontrolled access to the facility by unauthorized persons) compromise. If there is reason to believe the facility experienced a technical penetration or there is a greater threat to the facility or operation, commanders may request additional surveys.

1.5. The AF TSCM Program. The Under Secretary of Defense for Intelligence (USD(I)) authorizes the AF TSCM program per DoDI 5240.05. Headquarters (HQ) AFOSI centrally manages the program.

1.5.1. Customer-initiated requests for TSCM or AFOSI’s intelligence threat information will drive TSCM support to protect sensitive or classified AF information. In either case, AFOSI complies with DoDM 5240.01, Procedure 5, Part 4. **(T-0).**

1.5.2. The AF TSCM Program Manager must approve all AF personnel attending TSCM training specified in DoDI 5240.05. **(T-0).**

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Air Force Office of Special Investigations (AFOSI). The AFOSI is a field operating agency directly responsible to the Secretary of the Air Force (SecAF) for criminal investigative authority and is delegated the independent authority within the AF to initiate criminal investigations. The AFOSI Commander executes the USAF TSCM Program in accordance with Air Force Mission Directive (AFMD) 39, *Air Force Office of Special Investigations (AFOSI).*

2.1.1. The Program Manager for TSCM is located at HQ AFOSI, 27130 Telegraph Road, Quantico, VA, 22134.

2.1.2. AFOSI is the only AF organization with authorization to conduct TSCM activities, acquire and possess TSCM equipment, or maintain a staff of TSCM personnel.

2.1.3. TSCM Certification. TSCM personnel must meet the following TSCM certification requirements:

2.1.3.1. All initial and recurring training required in DoDI 5240.05. **(T-0).**

2.1.3.2. Have CI awareness training. **(T-1).**

2.1.3.3. Have counter surveillance training. **(T-1).**

2.1.3.4. Complete an initial AF or Red Cross certified Cardio Pulmonary Resuscitation and first aid course as well as refresher training every 2 years in accordance AFI 91-203, *Air Force Consolidated Occupational Safety Instruction*. **(T-1).**

2.1.3.5. Receive certification from the AF TSCM Program Manager. **(T-1).**

2.1.4. Under the direction and oversight of a certified TSCM specialist, other personnel may participate in TSCM activities.

2.2. The AFOSI Commander will:

2.2.1. Execute the AF TSCM Program in compliance with DoDI 5240.05. **(T-1).**

2.2.2. Ensure the AF TSCM Program meets the National TSCM mission objectives (see *The National Technical Surveillance Countermeasures Strategy of the United States of America*). **(T-1).**

2.2.2.1. Deter, detect, neutralize, and exploit adversarial technical surveillance capabilities directed against U.S. interests by employing proactive measures to the IC's advantage and anticipating future technical threats. **(T-1).**

2.2.2.2. Identify vulnerabilities and recommend actions by assessing and evaluating vulnerabilities and sharing information to address pervasive threats and vulnerabilities. **(T-1).**

2.2.2.3. Collaborate across disciplines to optimize TSCM efforts by seeking support from other national elements and providing support to other national elements.

2.3. AFOSI ICON Center will:

2.3.1. Oversee the operational execution of TSCM activities within the Air Force. **(T-2).**

2.3.2. Immediately notify the DoD TSCM program manager at Defense Intelligence Agency (DIA) of the discovery of a technical surveillance, in accordance with DoDI 5240.05. **(T-0).**

2.3.3. Notify the DoD TSCM program manager at DIA of other significant TSCM activities within one day. **(T-2).**

2.3.4. Prioritize TSCM activities based upon current, relevant threat information. **(T-2).**

2.3.5. Document TSCM reporting in the USD(I)-approved CI information system. **(T-0).**

2.4. The AF TSCM Program Manager will:

2.4.1. Serve as a senior AFOSI subject matter expert who represents the AF in working groups at the national-level for policy, research and development, telecommunications security, and any other groups chartered to address TSCM issues. **(T-2).**

2.4.2. Centrally manage the AF TSCM Program in accordance with DoDI 5240.05, DoDM S-5240.05, and DoDM 5240.01. **(T-2).**

2.4.3. Collaborate across disciplines (e.g., intelligence, security, law enforcement, science and technology, counterintelligence, etc.) to optimize TSCM efforts. **(T-2).**

2.4.4. Represent the AF at DoD and national-level TSCM forums. **(T-2).**

2.4.5. Submit TSCM technology requirements to the DoD's TSCM Information Management Group (TSCM-IMG). **(T-2).**

2.4.6. Submit TSCM training requirements and training curricula requirements to the TSCM-IMG annually. **(T-2).**

2.4.7. Ensure TSCM practitioners are trained and certified to conduct TSCM. **(T-2).**

2.4.8. Prioritize TSCM activities based upon current, relevant threat information. **(T-2).**

2.5. Air Force Commanders will:

2.5.1. Report to AFOSI any suspected technical surveillance activity per **Chapter 3** of this instruction. **(T-1).**

2.5.2. Request TSCM activities to ensure sensitive working environments are free of technical surveillance devices, identify hazardous conditions facilitating technical surveillance, identify conditions which are, or contribute to, technical security vulnerabilities, and employ countermeasures to defeat technical surveillance efforts. **(T-1).**

2.5.3. Employ OPSEC regarding any proposed, planned, in progress, or completed TSCM activities regarding a facility to prevent the compromise of TSCM tactics, techniques, and procedures. **(T-1).**

2.5.4. Request TSCM support from AFOSI. **(T-0).** Do not employ commercial TSCM activities, as such use may constitute a security compromise.

2.5.5. 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 and approval with the AF TSCM Program Manager. The AF component, working with AFOSI, will ensure only trained, qualified personnel operate the in-place monitoring equipment. Operate in-place monitoring equipment in accordance with DoDM 5240.01. **(T-0).**

Chapter 3

REPORTING SUSPECTED TECHNICAL SURVEILLANCE DEVICES OR ACTIVITIES

3.1. Overview. Upon discovery of suspected technical surveillance activities, all personnel will employ security measures in a manner preventing anyone at the "listening end" of the technical surveillance service from learning of the discovery. **(T-0).**

3.2. Actions upon Discovery.

3.2.1. Do not handle the device. Any person who discovers an actual or suspected technical surveillance device or possible technical surveillance activity must report it immediately to the person responsible for security of the area. **(T-1).** Discussion concerning the discovery shall not occur near the suspect device or activity and shall preferably occur outside the facility. AFOSI must treat all suspected technical surveillance devices or activities as possible intelligence gathering activities of a foreign intelligence service until proven otherwise. **(T-1).** AFOSI will classify the discovery in accordance with AFI 71-101, Volume 4, *Counterintelligence*; and DoDI C-5240.08, *Counterintelligence (CI) Security Classification Guide* (see Chapter 7 of this instruction for additional classification guidance). **(T-0).** Specific information necessary to facilitate the activity may be released to law enforcement agencies in accordance with DoDM 5240.01 and with the concurrence of the AF TSCM Program Manager. Upon device or suspected technical surveillance activity discovery, the security manager or person who finds it will:

3.2.1.1. Leave the suspect device in place and secure the area. Do not conduct tests or attempt removal unless under AFOSI direction after coordination with the AF TSCM Program Manager. **(T-1).**

3.2.1.2. Prevent any person without AFOSI authorization from tampering with or removing the device. **(T-1).**

3.2.1.3. Ensure no one discusses the suspect device in the area where it is located. **(T-1).**

3.2.1.4. Continue normal work in the area to the greatest extent possible. **(T-2).**

3.2.1.5. Brief only those people who are directly involved with the facility and must immediately know about the suspect device. **(T-2).**

3.2.1.6. Thoroughly document all aspects of the discovery noting location, dates, times, and all personnel involved or having knowledge of the discovery. **(T-2).**

3.2.2. As part of the official activity regarding the suspect device, only AFOSI agents may brief other individuals on a need-to-know basis, to include senior officials in the chain of command.

3.2.3. The person responsible for security of the area must immediately notify his/her supporting AFOSI unit or the AFOSI ICON Center Global Watch. **(T-2).** If needed, contact the AFOSI ICON Center Global Watch at 571-305-8484 (commercial) from outside the affected area via secure phone. Include the following information in the initial report **(T-0)**:

3.2.3.1. Name and contact information of the person reporting the suspected technical surveillance device.

3.2.3.2. Time and date of discovery.

3.2.3.3. Area, personnel, installation or facility involved.

3.2.3.4. Method of discovery.

3.2.3.5. Why you believe it may be a technical surveillance device.

3.2.3.6. An assessment/opinion as to whether or not personnel involved with the discovery alerted the "listener" or intended recipient of the potential compromise of their operation.

3.3. AFOSI ICON Center's Role:

3.3.1. After finding a suspected surveillance device, the AFOSI ICON Center must notify the DoD TSCM Program Manager within one duty day. **(T-0).**

3.3.2. The AFOSI ICON Center monitors AFOSI's TSCM activities.

3.3.3. AFOSI investigators will report events to the AFOSI ICON Center or to the national-level agencies as appropriate. **(T-2).**

3.4. AFOSI's Investigative Role upon Discovery of a Technical Surveillance Device. AFOSI will conduct TSCM activities following the discovery or alleged discovery of any technical surveillance device or activity targeting AF facilities, information, personnel or supported defense organizations. **(T-0).** Information derived from the activities can assist the intelligence community, evaluate damage to national security, provide current threat information to AF and supported commanders, and strengthen AF security and countermeasures programs.

3.5. AFOSI's Investigative Role upon Discovery of Network Surveillance Malicious Code. AFOSI will conduct detailed TSCM activities following the discovery or alleged discovery of any network surveillance malicious code, software, or activity targeting AF networks. TSCM agents shall report this discovery to the AFOSI ICON Center Cyber Division.

3.5.1. Upon discovery of a suspect nefarious network malicious code or software, do not stop the activity, but immediately notify the person responsible for network security for that particular network. Discussion concerning the discovery shall not occur in the area where other system administrators or network users are located. Preferably, it should occur outside the facility with a trusted network administrator (e.g., Communications Squadron Commander).

3.5.2. AFOSI must treat all suspected malicious network surveillance software, applications, services, or activities as possible intelligence gathering activities of a foreign intelligence service until proven otherwise. The TSCM team shall report this discovery to the AFOSI ICON Center Cyber Division.

Chapter 4

TSCM SUPPORT DURING CONFLICTS, CONTINGENCIES, OR SECURITY AND STABILITY OPERATIONS

4.1. Overview. This chapter identifies roles/responsibilities and establishes standard request and reporting procedures for TSCM support during conflicts, contingencies, or security and stability operations, in accordance with Joint Pub 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations*. DoDI 5240.16, *Counterintelligence Functional Services (CIFS)*, authorizes TSCM as a CI functional service. It is one of five separate, but interrelated functions within DoD CI (investigations, operations, collection, analysis and production, and functional services activities including, but not limited to TSCM, computer network operations, and polygraph).

4.2. Organization. In order to retain organizational integrity, a combined or joint force commander (JFC) normally exercises coordination authority of designated CI TSCM support elements through their respective Service component. Each CI organization's TSCM support element remains under the direction and control of their respective military Services and/or agency, unless the President or SecDef direct otherwise. If the President or SecDef directs, the JFC will exercise OPCON of military forces and capabilities (including TSCM) assigned and attached to the joint force (i.e. Joint CI units). **(T-0).** The JFC will not exercise OPCON over law enforcement or CI investigations. **(T-0).**

4.3. Roles and Responsibilities.

4.3.1. **Combined/Joint Force Commander (JFC).** The JFC is a combatant commander (CCDR), sub-unified commander, or joint task force commander. The CCDR exercises combatant command (COCOM) over a joint force. A sub-unified commander or joint task force (JTF) commander may receive authorization to exercise operational control (OPCON) or tactical control (TACON) over assigned forces.

4.3.2. **Joint Force Staff Counterintelligence and Human Intelligence Element (J2X).** As the command focal point for CI, the J2X is responsible to coordinate, synchronize, manage, and deconflict all DoD CI activities in the JFC's operational area.

4.3.3. **Task Force Counterintelligence Coordination Authority (TFCICA).** Upon designation, the TFCICA is the CI agent who exercises coordinating authority over joint CI mission requirements in a designated joint operations area. Should this coordinating authority not prove sufficient to accommodate the JFC CI goals, the TFCICA then refers the matter to the JFC with sufficient command authority to resolve the situation. Typically this JFC is the CCDR who exercises COCOM over assigned CI activities and units in the joint operations area (JOA). The TFCICA also coordinates and deconflicts the activities of the Military Department Counterintelligence Organization (MDCO) component CI organizations in the JOA. The JFC may also delegate tasking authority to the TFCICA. The TFCICA will engage with the senior representative of each Service CI element in the operational area as the composition of the staff is determined to ensure the Services' contribution reflects their proportionate share of CI resources in the operational area. This is normally in the CI component's best interest, since their own personnel are most knowledgeable about their capabilities and limitations, and can ensure appropriate apportionment of their component during the contingency.

4.3.4. **Operations Support Element (OSE).** The OSE (if established by the J2X) consists of three separate branches and is responsible for all administrative, operations support, and services support functions within the J2X. TSCM is aligned under the Technical Support Branch along with Polygraph, Biometrics, Linguists and Technical Operations.

4.3.5. **Command Counterintelligence Coordinating Authority (CCICA).** The CCICA is the combatant commander's expert on CI matters. The CCICA exercises staff supervision over subordinate joint CI staff elements on behalf of the combatant commander to maintain complete situational awareness of all CI activities throughout the combatant command assigned to the operational area.

4.3.6. **Military Departments or Service CI Organizations.** Service CI organizations (e.g., AFOSI) are responsible for the conduct, direction, management, coordination, and control of CI activities within their respective organization, as well as providing CI support to other organizations as required.

4.3.7. **DoD TSCM Program Manager (PM).** The PM at DIA coordinates TSCM responsibilities when Military Service CI organization are unavailable or when it's unclear which Military Service CI organization has primary TSCM responsibility.

4.4. Request and Reporting Procedures.

4.4.1. All AF units assigned to the joint operations area will request TSCM through the J2X or their designee. **(T-0).** The J2X ensures requests are in accordance with DoDM 5240.01, DoDI 5240.05, ICD 304, and ICD 310. AFOSI commanders will conduct TSCM activities in accordance with DoDM S-5240.05. **(T-0).** Delegation of this responsibility can be made to the TFCICA (if assigned) or operations support element (OSE) (if assigned).

4.4.2. Unless otherwise designated by the J2X, AF units in the JOA should use AF Form 4445, *Request for Technical Surveillance Countermeasures (TSCM)*, or the TSCM request format in DoDM S-5240.05 to request TSCM.

4.4.3. J2X should receive, or TFCICA if the J2X should designate, all TSCM requests from units in the JOA. Any request misrouted to a Service CI organization should be forwarded to the J2X for action (ref. **Attachment 2**, JOA TSCM Request Flowchart).

4.4.4. The J2X, validates/approves the request in accordance with DoD policy and coordinates support as follows:

4.4.4.1. If the combatant commander determines the formation of a joint CI unit(s) with focus on both strategic and operational-level CI missions would make CI support (all or designated functions) more responsive to command needs, then the CI unit(s) may have dedicated TSCM personnel. The CI unit will define the full scope of responsibility and authority in the unit's concept of operations (CONOPS). **(T-0).** If TSCM capabilities are resident in the command's joint CI unit(s), the TFCICA shall coordinate the TSCM activity with this supporting joint CI unit (in accordance with the unit's CONOPS) once the J2X validates the request.

4.4.4.2. If there is no joint CI unit with TSCM capability, or if there is a requirement for additional TSCM resources to support the JFC within an operational area, the TFCICA should coordinate through the combatant command CCICA and sister elements within the J2X for Military Service CI component TSCM support. The Service CI components will provide CI TSCM support to their Service component commanders, combatant commanders, designated task forces, the Chairman of the Joint Chiefs of Staff (CJCS), and other DoD agencies and defense support activities in accordance with DoDI 5240.05, Enclosure 3; using the TSCM capabilities through their own organizations or other military support agencies. **(T-0).**

4.4.4.3. In addition to the Military Service CI components, additional DoD organizations with TSCM resources exist and may be available to provide limited support. TSCM support from these organizations should be coordinated through the DoD TSCM PM at DIA.

4.4.5. The joint CI unit or Service CI organization conducting the TSCM shall be responsible for reporting TSCM activities in accordance with established DoDI 5240.05. **(T-0).**

4.4.6. The TSCM team lead for TSCM activities outside the U.S. on other than a U.S.-controlled installation must coordinate activities in accordance with ICD 304 and ICD 310 as appropriate. **(T-0).**

4.4.7. Reference Military Service TSCM organization MOUs as applicable.

Chapter 5

TSCM ACTIVITIES

5.1. Overview. Reference **Chapter 4** of this instruction for requesting support during conflicts, contingencies, or security and stability operations. TSCM activities are highly specialized CI activities and as such, are particularly vulnerable to compromise. Therefore, consider all reasonable measures to ensure there is no compromise of the request for the TSCM activities and subsequent activity. Until the activity indicates otherwise, assume the facility is under technical surveillance. Therefore, any discussion of the TSCM activities in the area could compromise it and result in the surveillance device's temporary deactivation or removal. The TSCM PM will not approve requests for TSCM activities via non-secure means and will consider such requests compromised.

5.1.1. AFOSI may conduct pre-construction surveys as a service to AF Commanders who are designing secure areas for the protection of sensitive and/or classified information. Organizations planning major new classified projects or programs should consider the need for TSCM activities early in the process.

5.1.2. TSCM personnel are authorized access to the content of any communications acquired during the TSCM activity in accordance with DoDM 5240.01.

5.1.3. Prior to AFOSI conducting TSCM activities where classified meetings or conferences occur outside an appropriately cleared U.S. Government facility or a cleared U.S. contractor facility, SAF/AA must approve an exception to policy, in accordance with AFI 16-1404, *Air Force Information Security Program*; DoDM 5200.01, Volume 3, *DoD Information Security Program*; and DoDI 5240.05. **(T-0).**

5.1.4. At a minimum, all AFOSI TSCM personnel have a Top Secret security clearance with Sensitive Compartmented Information access. Requestors are responsible for providing the appropriate access authorization necessary for unescorted access of TSCM personnel. TSCM personnel cannot appear out of place and should be indistinguishable from other permanent facility personnel.

5.2. Discussing the TSCM Request and Activities. Never discuss the TSCM request and/or activities within the survey area or with foreign nationals. Should a surveillance device exist, such a discussion would most likely lead to device removal prior to the TSCM activities and later reinstallment, or simply switched off remotely. Under such circumstances, the probability of discovering the device diminishes. For this reason, no discussion or verbal comments concerning the pending support should occur in the survey areas.

5.3. TSCM Support during Exercise and Deployments. Units can request TSCM activities to support exercises involving sensitive or classified information; however, they are never part of an exercise. The only exceptions are training operations conducted by the intelligence community or AFOSI for the specific purpose of evaluating the effectiveness of TSCM equipment, procedures, or personnel. The AFOSI ICON Center will approve participation in these exercises. **(T-2).**

5.4. Authorized Requestors. AF or DoD entities responsible for areas where the processing or discussion of classified or sensitive information occur may submit requests for TSCM activities. Non-AF agencies requesting support from AFOSI will abide by this instruction as a condition for AFOSI approval. **(T-2).** Failure to follow AFOSI's guidance during an on-going TSCM activity may result in its termination.

5.5. Request Process. Follow the instructions below to request TSCM via secure communications. Units should not make requests from within the facility of concern.

5.5.1. Submit requests to local or servicing AFOSI unit using AF Form 4445. If unable to determine the servicing AFOSI unit, contact the AFOSI ICON Center Global Watch's Hotline at 571-305-8484 via secure means from outside of the area of concern.

5.5.2. The Air Force Program Security Manager must coordinate TSCM requests for a Special Access Program (SAP).

5.5.3. TSCM may involve the incidental acquisition of the nonpublic communication of U.S. persons without their consent. The official in charge of the facility, organization, or installation must consent to the use of TSCM in accordance with where the countermeasures are to be undertaken (ref. DoDM 5240.01). **(T-0).** Within the AF, this is usually the commander (or equivalent), not the unit security officer or staff members.

5.6. Approval Criteria for TSCM. Not all facilities processing sensitive and/or classified material can receive TSCM support. AFOSI will use a risk-based approached to planning and executing the Air Force TSCM program. **(T-1).**

5.6.1. AFOSI retains final approval for the conduct of TSCM activities.

5.6.2. AFOSI must coordinate TSCM activities outside the U.S. on other than a U.S.-controlled installation with the DNI in accordance with ICD 304 and ICD 310. **(T-0).**

5.6.3. New facilities and those having undergone major renovations cannot receive TSCM support until completion of all construction and interior decoration/finishing, all equipment and furnishing are in place and the facility is fully operational and working on a normal day-to-day functional status. AFOSI ICON Center may waive the requirement under certain circumstances such as when the threat is extremely high or the information of concern is extremely sensitive (i.e., related to loss of life).

5.6.4. General officers' or other senior officials' quarters, offices, and conveyances, because of their position and potential targeting, may receive TSCM support despite minimal security provisions.

5.6.5. Normally, once a facility receives TSCM activities it cannot receive recurring TSCM activities. In principle, once an area has been the subject of a TSCM activity with a favorable outcome, the results are considered valid as long as the security integrity of the facility is maintained. AFOSI will recommend in its final report if additional or recurring TSCM support should be considered by the commanding official. **(T-1).**

5.6.6. AFOSI may approve follow-on TSCM support if:

5.6.6.1. There is evidence to suggest an area's technical penetration.

5.6.6.2. There was extensive construction, renovation or structural modifications requiring unescorted access by uncleared individuals.

5.6.6.3. Unauthorized personnel gained uncontrolled or unescorted access to the secure area. If this access was a result of poor security practices, units must implement corrections before AFOSI will consider follow-on TSCM activities.

5.6.7. AFOSI ICON Center may designate recurring TSCM support for certain high profile areas, due to extensive FIE targeting.

5.7. Scheduling. TSCM activities are not inspections. No preparations are necessary other than those outlined in this instruction. AFOSI will coordinate scheduling with the requestor. However, a specific date cannot be set.

5.7.1. The requestor is given a 90-day window for the TSCM activity. After scheduling, knowledge of a pending TSCM activity is kept on a need-to-know basis. TSCM activities announced in advance, lose their effectiveness.

5.7.2. AFOSI cannot schedule TSCM activities when the facility is empty or not performing its primary function. For example, AFOSI should not schedule activities involving senior officer suites if the officer is away. Adversaries would likely turn off or disable surveillance devices in the area making its discovery problematic.

5.8. Technical Security Measures. Units considering TSCM for an area should take the following security measures to help ensure the area is not vulnerable to technical surveillance. Units should consider the following measures prior to requesting TSCM:

5.8.1. Ensure the telephone security in the area of concern is in accordance with Committee for National Security Standards (see: **http://www.cnss.gov/**).

5.8.2. Ensure adequate acoustical protection exists to prevent unauthorized persons from overhearing discussion in the area.

5.8.3. Ensure necessary physical security safeguards are in place to prevent unauthorized access to the area.

5.8.4. Remove all electronic storage or recording equipment not certified as essential to the mission.

5.8.5. Provide properly trained escorts for those persons who need occasional access to the facility but who do not meet the criteria for unescorted access.

5.8.6. Do not allow repairs or alteration of sensitive areas except under the supervision of qualified and responsible personnel who can control the workers.

5.8.7. Minimize the introduction of new furnishings or equipment that have not been under US control or procured through secure means.

5.8.8. Do not allow personal electronic devices or portable electronic devices (e.g., cell phones) in sensitive or classified discussion or processing areas.

5.9. Unit Responsibilities Before, During and After a TSCM. The organization's Commander requesting TSCM must take steps to ensure the TSCM team is not compromised when preparing for or conducting the TSCM activity. **(T-2).** Accordingly, the requestor will ensure the following:

5.9.1. Ensure the team members have unescorted access to the entire facility during the TSCM activity. **(T-1).** This includes all information systems, including telephones, classified and unclassified networks, teleconference systems, etc. (ref. DoDM S-5240.05). Commanders will identify and make system administrators available to TSCM personnel, as needed. **(T-1).**

5.9.2. Ensure the team is able to transport their equipment into the facility and properly secure it without undue attention. TSCM equipment consists of items not normally allowed within secured classified environments (e.g., cameras, recording and transmitting equipment, network inspection equipment, and other types of electronic devices). This equipment is authorized solely for TSCM purposes and is not subject to inspection, validation, or pre- approval by unit personnel.

5.9.3. Maintain a normal working atmosphere in the area before and during a TSCM activity. This includes refraining from any comments in the area which would reveal a TSCM activity is contemplated or underway. **(T-2).**

5.9.4. For a Sensitive Compartmentalized Information Facility (SCIF), provide the automated information system accreditation package including local area network maps to the TSCM team when requested.

5.9.5. Provide a copy of the facility blueprints and/or floor plans when requested. **(T-2).**

5.9.6. Ensure the establishment of continuous access controls as part of an effective security program to preclude undetected unauthorized access. **(T-2).**

5.9.7. Ensure only those people with an absolute need-to-know learn there is an activity request or actual activity is underway. **(T-2).**

5.9.8. Do not compromise TSCM activity by allowing uncleared visitors into the area while the activity is underway. **(T-2).**

5.9.9. If, in the opinion of the TSCM team leader, there is a compromise in the effectiveness of the TSCM activity, the team leader will terminate the activity and not reschedule until correction of the situation causing the compromise. **(T-1).** The unit's commander will initiate an appropriate security inquiry if the compromise involves disclosure of classified information to uncleared personnel. **(T-2).**

5.10. TSCM Activity Out-Briefings. At the conclusion of the activity, the TSCM team should provide a briefing on the results of the TSCM activity to appropriate facility personnel. The purpose of the briefing should be to make the requestor aware of any security deficiencies discovered during the activity. The TSCM team leader will provide recommendations for corrective measures to enhance information security. **(T-0).** The TSCM team leader will include all applicable deficiencies and recommendations in the TSCM written report provided to the requesting official no later than 30 duty days after completion. **(T-0).** At the discretion of the TSCM team, minor deficiencies corrected during the activity by facility personnel may not be included in the report.

5.11. What to Expect from TSCM. The TSCM team leader will identify unauthorized technical surveillance and indicate the technical security status of the inspected area during the period of the activity. **(T-0).** The activity provides the requester with a professional evaluation of a facility's technical security posture. These evaluations are appropriate for virtually any area where discussion or processing of classified or sensitive information occurs on a routine basis. However, TSCM is a manpower and resource-intensive activity and only for those facilities where there is a viable threat. Furthermore, TSCM activity cannot replace traditional security measures as its focus is primarily counterintelligence, not security or administrative compliance. Failure to maintain the physical security of the area likely nullifies any previous assurance from the TSCM team that the area is free of technical surveillance devices. The TSCM teams:

5.11.1. Detect any technical surveillance exploitation of an area, usually through the discovery of a technical surveillance device or modification of installed equipment.

5.11.2. Identify classified or sensitive information "leaking" from a facility. Note: TSCM is not a replacement for Emissions Security (EMSEC) or TEMPEST measures (for EMSEC program information, see: AFSSI 7700, *Communications and Information, Emission Security*).

5.11.3. Identify exploitable security conditions supporting or facilitating the installation of a device or modification of existing equipment to conduct technical surveillance.

5.11.4. DoDM 5240.01 authorizes AFOSI agents performing TSCM activities to monitor all government communications systems within or servicing the area. DoDM 5240.01 further authorizes AFOSI agents to collect signals and communications from any device or system servicing the area (authorized or unauthorized) to determine its existence and assess its capacity for electronic surveillance. DoDM 5240.01, Procedure 5 contains the limitations to this monitoring. AFOSI agents will monitor these systems (e.g., traditional phone systems, voice-over- internet- protocol, networks, etc.) by physical, electronic, or other means DoDM S-5240.05. **(T-0).**

5.12. Requesting Technical Security Threat Briefings. Awareness training of the technical threats is an integral part of the TSCM program. AFOSI can provide CI threat briefings to educate AF personnel on best practices and procedures to minimize the threat of foreign collection activities.

5.12.1. Upon request, AFOSI will present appropriately classified briefings on current technical security threats and TSCM procedures to the following personnel:

5.12.1.1. Personnel who are responsible for the security of sensitive facilities. **(T-2).**

5.12.1.2. Personnel assigned to sensitive facilities receiving TSCM activities. **(T-2).**

5.12.1.3. Personnel who provide escort for uncleared visitors or workers in areas eligible for TSCM activities. **(T-2).**

5.12.2. Individuals or offices desiring technical security threat briefings should send written requests containing the following information to their servicing AFOSI unit:

5.12.2.1. The name of the organization or the activity requesting the briefing.

5.12.2.2. A brief mission synopsis of the organization or activity.

5.12.2.3. The location for the requested briefing.

5.12.2.4. The approximate number of individuals attending the briefing, their level of security clearance, and a brief synopsis of their positions within the organization (such as command staff, security management, etc.).

5.12.2.5. A preferred briefing date.

5.12.2.6. All requests should be sent as far in advance of the briefing as possible to allow for the collection of current relevant threat information.

Chapter 6

TSCM REPORTS

6.1. Overview. The TSCM team leader will generate TSCM reports using the DoD standard report format and comply with all requirements in DoDI 5240.05. **(T-0).**

6.1.1. The report needs to include threat assessments used to prioritize the activity and any factors used to determine the overall security posture of the area.

6.1.2. Reports of TSCM activities conducted within temporary facilities in a deployed environment may be limited in scope and forwarded via message or other secure means.

6.2. TSCM Report Dissemination. AFOSI will submit a written TSCM report to the requestor within 30 duty days of the conclusion of the TSCM activities. **(T-3).**

6.2.1. TSCM reports should reflect only those conditions with the potential to allow the transmittal of information to unauthorized persons through technical and physical penetrations or deficiencies in the facility. The report provides recommendations for correcting the deficiencies, but are not directive in nature.

6.2.2. Commanders receiving TSCM reports will not disseminate the reports without the permission of the AF TSCM Program Manager. **(T-1).** Commanders may disseminate unclassified excerpts to assist in correcting identified deficiencies. These excerpts cannot divulge a TSCM activity discovering the deficiency, a connection to AFOSI, or the significance of the security deficiency. ****EXCEPTIONS*:** A copy of the report on any TSCM activity conducted in a DIA certified SCIF should be available to DIA/DAC-2 (DIA Chief, Security Division). TSCM reports are also archived in Portico and available to CI personnel with the appropriate clearance and access (i.e., analysts and DoD TSCM personnel).

6.3. Required Actions Upon Receipt of the Report. TSCM activities are not for the purpose of determining compliance with administrative security requirements. The requesting unit commander must forward an after action report to AFOSI within 90 calendar days of receipt of a report if the TSCM identified any security vulnerabilities or items of security interest, in accordance with DoDI 5240.05. **(T-0).** The requestor will provide an appropriately classified after action report to the AFOSI point of contact for the TSCM activity. **(T-0).** After action reports are essential to measure the effectiveness and value of the DoD TSCM Program.

6.3.1. The TSCM team leader's report will include all actions taken to correct identified items and include the following:

6.3.1.1. The security vulnerabilities and items of security interests corrected using the recommendations contained in the TSCM report. **(T-0).**

6.3.1.2. The security vulnerabilities and item of security interests corrected using recommendations other than those provided in the TSCM report. **(T-0).**

6.3.1.3. The rationale and acceptance of risk for any security vulnerability or item security interests not corrected. **(T-0).**

6.3.2. Failure to submit an after action report may preclude further TSCM activities at the facility or program.

6.3.3. There is no requirement for an after action report for TSCM activities on temporary facilities in a deployed environment.

Chapter 7

HANDLING TSCM INFORMATION

7.1. Classification of TSCM Information. Information pertaining to the TSCM program is protected to preserve the integrity of the information and the program. Use DoDI C-5240.08; Executive Order 13526, *Classified National Security Information*; and DIA's *DoD Technical Surveillance Countermeasure (TSCM) Security Classification Guide*, to determine the classification level.

7.1.1. If the TSCM activity is associated with a SAP, the classification guidance for that program may also apply.

7.1.2. Do not normally classify photographs, floor plans, or other diagrams of the facility unless they are specifically associated with the TSCM activity.

7.2. Compromise of TSCM Information. AFOSI agents will report any compromise of classified TSCM information to unauthorized persons (i.e., foreign nationals or personnel lacking the proper security clearance) immediately to the AF TSCM Program Manager. **(T-1).** AFOSI will document the details of the compromise and/or monitor any subsequent investigation into the compromise. The AF TSCM Program Manager will in-turn provide the findings to DIA (DoD TSCM Program Manager) for damage assessment. **(T-1).**

7.3. Information Release. Requests for release of any information, classified or unclassified, pertaining to Air Force TSCM information, methods, or equipment are to be forwarded to the AF TSCM Program Manager.

7.4. TSCM Equipment Procurement. Do not associate information relating to the acquisition or procurement of any equipment (U.S. Government or commercial off-the-shelf systems) for supporting TSCM activities with AFOSI or the AF TSCM program.

7.4.1. Only solicit for procurement of TSCM equipment with DoD TSCM-IMG vetting and approval.

7.4.1.1. Upon vetting and approval, advertise the requirements for equipment supporting the AF TSCM Program as Brand Name only in accordance with the Federal Acquisition Regulation (FAR), Part 6, *Competition Requirements*, current edition. See Title 10 United States Code Section 2304(c)(1), *Contracts: competition requirements*; FAR, Part 6; and Defense FAR Supplement (DFARS), current edition, for additional information.

7.4.1.2. Solicit offers from as many U.S. potential sources as deemed possible.

SAMI D. SAID, Lieutenant General, USAF
The Inspector General

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMD 39, *Air Force Office of Special Investigations (AFOSI)*, 7 May 2015

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 13 November 2015

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 71-101 Volume 4, *Counterintelligence*, 26 January 2015

AFI 91-203, *Air Force Consolidated Occupational Safety Instruction*, 15 June 2012

AFMAN 33-363*, Management of Records*, 1 March 2008

AFSSI 7700, *Communications and Information, Emission Security*, 24 October 2007 (IC 14 Apr 09)

DFARS 206.302-1, *Other Than Full and Open Competition*

DoD Instruction C-5240.08*, Counterintelligence (CI) Security Classification Guide*, 28 November 2011

DoD Instruction 5240.05, *Technical Surveillance Countermeasures (TSCM)*, 3 April 2014

DoD Instruction 5240.16, *Counterintelligence Functional Services (CIFS)*, 27 August 2012

DoD Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012

DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 August 2016

DoDM S-5240.05, *The Conduct of Technical Surveillance Countermeasures, 23 April 2015*

DoD Technical Surveillance Countermeasure (TSCM) Security Classification Guide, Version 1, 19 July 2016

Executive Order 13526, *Classified National Security Information*, 29 December 2009

FAR 6.302-1, *Other Than Full and Open Competition*

Intelligence Community Directive 304, *Human Intelligence*, 9 July 2009

Intelligence Community Directive 310, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States*, 27 June 2016

Intelligence Community Directive 702, *Technical Surveillance Countermeasures*, 18 February 2008

Joint Publication 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations*, 16 March 2011

The National Technical Surveillance Countermeasures Strategy of the United States of America, 2008

Title 10 United States Code Section 2304*, Contracts: competition requirements*

Prescribed Forms

AF Form 4445*, Request for Technical Surveillance Countermeasures (TSCM)*

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMD—Air Force Mission Directive

AFPD—Air Force Policy Directive

AFOSI—Air Force Office of Special Investigations

ANG—Air National Guard

CAP—Civil Air Patrol

CCDR—Combatant Commander

CCICA—Command Counterintelligence Coordinating Authority

CI—Counterintelligence

CJCS—Chairman of the Joint Chiefs of Staff

COCOM—Combatant Command

CONOPS—Concept of Operations

DFARS—Defense Federal Acquisition Regulation Supplement

DIA—Defense Intelligence Agency

DNI—Director of National Intelligence

DoD—Department of Defense

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

EMSEC—Emissions Security

FAR—Federal Acquisition Regulation

FIE—Foreign Intelligence Entity

HQ—Headquarters

IC—Intelligence Community

ICD—Intelligence Community Directive

ICON—Investigations, Collections, Operations Nexus

J2X—Joint Force Staff Counterintelligence and Human Intelligence Element

JFC—Joint Force Commander

JTF—Joint Task Force

JOA—Joint Operations Area

MDCO—Military Department Counterintelligence Organization

MOU—Memorandum of Understanding

OPCON—Operational Control

OPR—Office of Primary Responsibility

OPSEC—Operational Security

OSE—Operations Support Element

PM—Program Manager

SAP—Special Access Program

SecAF—Secretary of the Air Force

SCIF—Sensitive Compartmented Information Facility

TACON—Tactical Control

TFCICA—Task Force Counterintelligence Coordination Authority

TSCM—Technical Surveillance Countermeasures

TSCM-IMG—Technical Surveillance Countermeasures Information Management Group

USD(I)—Under Secretary of Defense for Intelligence

Terms

Approval Authority—Senior leader responsible for contributing to and implementing policies and guidance/procedures pertaining to his/her functional area(s) (e.g., heads of functional two-letter offices).

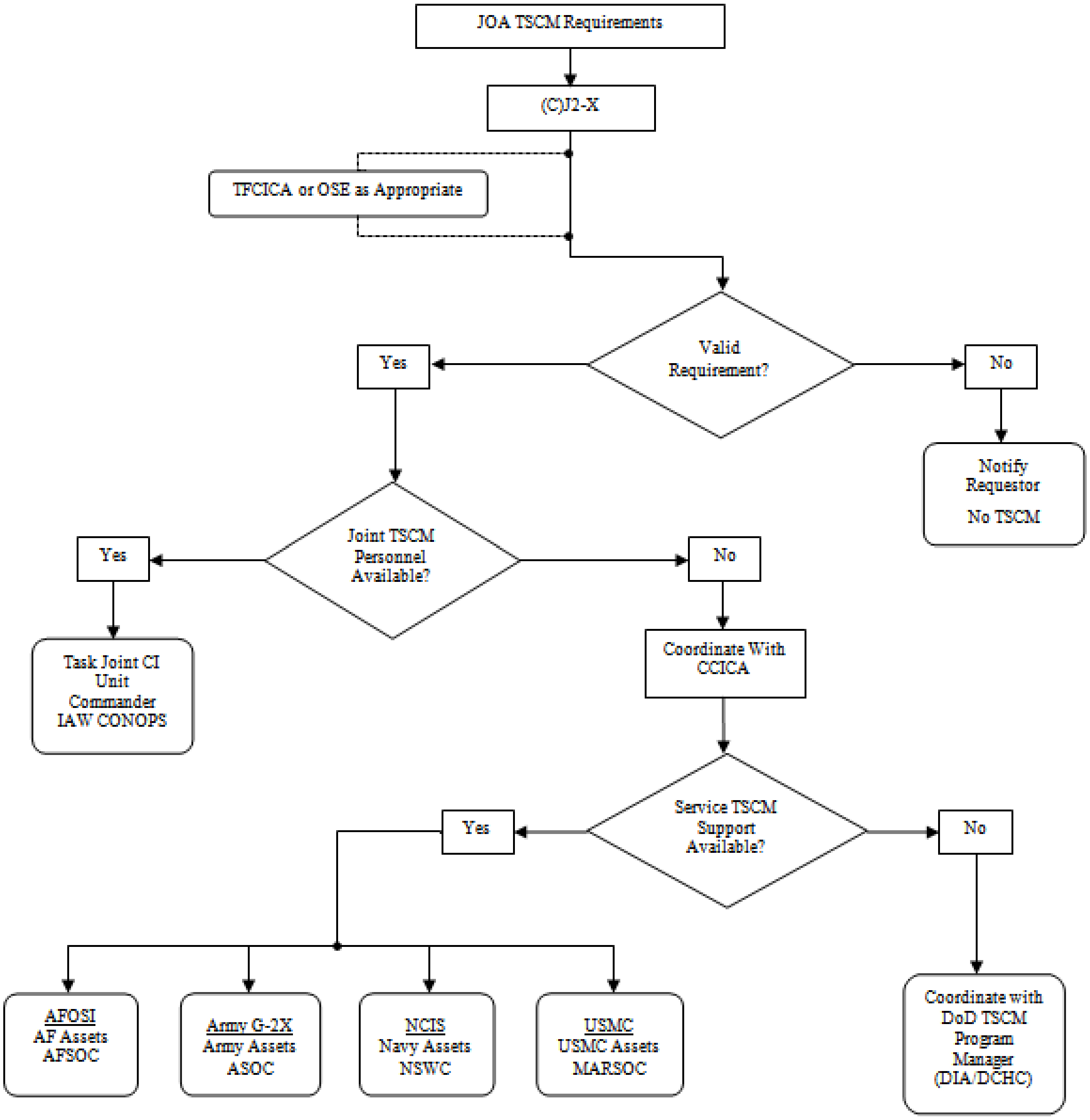
Portico—An automated information management system that serves as the Community's designed system for all CI reporting within the Department of Defense.

TEMPEST—An unclassified term referring to technical investigation for compromising emanations from electrically operated processing equipment. This term is synonymous with EMSEC.

Attachment 2

JOINT OPERATIONS AREA TSCM REQUEST FLOWCHART

Figure A2.1. Joint Operations Area TSCM Request Flowchart.


JOA TSCM Requirements
(C)J2-X
TFCICA or OSE as Appropriate
Valid Requirement?
Yes
No
Notify Requestor No TSCM
Joint TSCM Personnel Available?
Yes
No
Task Joint CI Unit Commander IAW CONOPS
Coordinate With CCICA
Service TSCM Support Available?
Yes
No
AFOSI AF Assets AFSOC
Army G-2X Army Assets ASOC
NCIS Navy Assets NSWC
USMC USMC Assets MARSOC
Coordinate with DoD TSCM Program Manager (DIA/DCHC)