Headquarters
Department of the Army
Washington, D.C.
3 October 1986

*Army Regulation 381-14

Effective 3 November 1986

Military Intelligence (U)

Technical Surveillance Countermeasures (TSCM) (U)

This UPDATE printing publishes a revision which is effective 3 November 1986. Because the structure of the entire revised text has been reorganized, no attempt has been made to highlight changes from the earlier regulation dated 26 November 1976.

By Order of the Secretary of the Army:

JOHN A. WICKHAM, JR.
General, United States Army
Chief of Staff

Official:
R.L. DILWORTH
Brigadier General, United States Army
The Adjutant General

(U) Summary. This regulation implements DOD Instruction 5240.5, 23 May 1984. It describes the U.S. Army TSCM program, objectives, purpose, and scope, and sets forth policies; it describes responsibilities for administration of the program; it describes procedures for requesting, and provides validation of, TSCM support; it directs reporting procedures for discovery of technical surveillance devices; and explains selection, training, utilization, and operational security requirements for TSCM special agents.

(U) Applicability. The regulation is applicable to the Active Army, and the United States Army Reserve (USAR). It applies to the Army National Guard (ARNG) only when in a federalized status.

(U) Impact on New Manning System. This regulation does not contain information that affects the New Manning System.

(U) Internal control systems. This regulation is not subject to the requirements of AR 11-2. It does not contain internal control provisions.

(U) Supplementation. Supplementation of this regulation and establishment of forms other than DA forms are prohibited, without prior approval from HQDA (DAMI-CIC), WASH DC, 20310-1054.

(U) Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

(U) Suggested improvements. The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence (OACSI). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIC), WASH DC, 20310-1054.

(U) Distribution. Distribution of this issue has been made in accordance with DA Form 12-9C-R requirements for 381-series publications. The number of copies distributed to a given subscriber is the number of copies requested in Block 1033 of the subscriber's DA Form 12-9C-R.

(U) Contents (Listed by paragraph number)

*This regulation supersedes AR 381-14, 26 November 1976

Headquarters
Department of the Army
Washington, D.C.
3 October 1986

*Army Regulation 381-14

Effective 3 November 1986

Military Intelligence (U)

Technical Surveillance Countermeasures (TSCM) (U)

This UPDATE printing publishes a revision which is effective 3 November 1986. Because the structure of the entire revised text has been reorganized, no attempt has been made to highlight changes from the earlier regulation dated 26 November 1976.

By Order of the Secretary of the Army:

JOHN A. WICKHAM, JR.
General, United States Army
Chief of Staff

Official:
R.L. DILWORTH
Brigadier General, United States Army
The Adjutant General

(U) Summary. This regulation implements DOD Instruction 5240.5, 23 May 1984. It describes the U.S. Army TSCM program, objectives, purpose, and scope, and sets forth policies; it describes responsibilities for administration of the program; it describes procedures for requesting, and provides validation of, TSCM support; it directs reporting procedures for discovery of technical surveillance devices; and explains selection, training, utilization, and operational security requirements for TSCM special agents.

(U) Applicability. The regulation is applicable to the Active Army, and the United States Army Reserve (USAR). It applies to the Army National Guard (ARNG) only when in a federalized status.

(U) Impact on New Manning System. This regulation does not contain information that affects the New Manning System.

(U) Internal control systems. This regulation is not subject to the requirements of AR 11-2. It does not contain internal control provisions.

(U) Supplementation. Supplementation of this regulation and establishment of forms other than DA forms are prohibited, without prior approval from HQDA (DAMI-CIC), WASH DC, 20310-1054.

(U) Interim changes. Interim changes to this regulation are not official unless they are authenticated by The Adjutant General. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

(U) Suggested improvements. The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence (OACSI). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIC), WASH DC, 20310-1054.

(U) Distribution. Distribution of this issue has been made in accordance with DA Form 12-9C-R requirements for 381-series publications. The number of copies distributed to a given subscriber is the number of copies requested in Block 1033 of the subscriber's DA Form 12-9C-R.

(U) Contents (Listed by paragraph number)

*This regulation supersedes AR 381-14, 26 November 1976

Chapter 1
(U) General Information (U)

1-1. (U) Purpose

(U) This regulation implements Department of Defense (DOD) Instruction 5240.5, dated 23 May 1984, and prescribes Department of the Army policy concerning the TSCM program.

1-2. (U) References

(U) Required and related references and referenced forms are listed in appendix A.

1-3. (U) Explanation of abbreviations and terms

(U) Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. (U) Objectives

(U) Technical surveillance devices have been discovered in U.S. facilities worldwide. These finds clearly demonstrate the existence of a technical surveillance threat to sensitive classified defense information. The objectives of the TSCM program are—

a. (U) To provide a systematic and effective program for the detection and nullification of technical surveillance penetrations, technical surveillance hazards, and physical security weaknesses.

b. (U) To provide responsible Army commanders and managers with guidelines for the enhancement of security and reduction of the vulnerability of sensitive areas to the technical surveillance threat.

1-5. (U) Threat

(U) The technical threat is posed by the capability of all foreign intelligence or dissident domestic agents to use technical surveillance means to collect information from sensitive U.S. facilities and activities or against select targeted individuals. The threat usually takes the form of devices installed or employed at the direction of a foreign power for the specific purpose of audio, visual, or emanation collection of information from within a sensitive area. This information may be obtained by direct technical penetration, or by exploiting a technical surveillance security hazard or physical security weakness in a sensitive area.

1-6. (U) TSCM program functions

(U) Technological advances make the detection of technical surveillance devices and technical security hazards so difficult that, in most cases, their discovery is possible only by highly trained personnel using specialized techniques and equipment. The TSCM program includes all measures taken to reduce the vulnerability of sensitive areas to the technical surveillance threat. These security measures include four distinct, interdependent functions, each of which has a direct bearing on the effectiveness of the overall program, as outlined below.

a. (U) *Detection.* TSCM surveys, inspections, and penetration investigations of sensitive areas are counterintelligence (CI) investigations designed to detect the presence of technical surveillance devices, technical security hazards, or physical security weaknesses which would permit the technical or physical penetration of the facility. TSCM services are time consuming and costly and will be of no lasting value if the area serviced is not maintained under effective physical and technical security controls. Occupants of sensitive areas share a responsibility in detection in that they should recognize and report new or unusual objects or conditions.

b. (U) *Nullification.* This includes measures, both active and passive, to neutralize or negate technical devices which may be employed, or to make the placement of such devices more difficult.

(1) (U) Passive nullification can be accomplished by such techniques as—

(a) (U) Soundproofing sensitive areas to include air-conditioning and heating ducts.

(b) (U) Removing telephones and intercommunications systems or installing protective devices on those items which cannot be removed.

(c) (U) Removing excess and unused wiring.

(d) (U) Securing and inspecting utility tunnels and crawl spaces adjacent to sensitive areas.

(e) (U) Using noise generators or music to mask sensitive conversations.

(2) (U) Active nullification is accomplished by detecting and removing or exploiting discovered technical surveillance devices.

c. (U) *Isolation.* The establishment of special areas for the conduct of activities involving sensitive information, and the exclusion or close control of all uncleared personnel in that area, can reduce vulnerability to the technical surveillance threat. This may involve isolation of an entire building or designation of smaller special areas with appropriate physical and other security barriers or controls.

d. (U) *Education.* The education of all personnel concerning the threat of technical surveillance and the part the individual plays in the U.S. Army TSCM program is vital. Individuals must be made aware of the nature of the technical surveillance threat and the part that they can play in the TSCM program. Personnel should be alert for unusual conditions such as strange electronic equipment or components, recently installed equipment or fixtures to include non-electrical or electronic items which were not requested or are not needed, or the unusual performance of communications equipment. They should be trained to check the identification of repair and maintenance service personnel, and to discuss sensitive information only in approved designated areas.

Chapter 2
(U) TSCM Investigations and Support (U)

Section I
(U) Responsibilities (U)

2-1. (U) The Assistant Chief of Staff for Intelligence, DA (ACSI, DA)

(U) The Assistant Chief of Staff for Intelligence, Department of the Army will—

a. (U) Monitor and provide general staff supervision of U.S. Army TSCM programs and operations.

b. (U) Develop Army TSCM policies, procedures, and regulatory guidance.

c. (U) Provide or assign Army representatives to national level interagency committees and their working groups to coordinate information on research and development efforts, TSCM equipment and techniques, finds, hazards, and other items of mutual interest that benefit members of the U.S. Intelligence Community.

d. (U) Establish Army requirements for research, development, testing, and evaluation programs for TSCM material to ensure that the Army TSCM program adequately counters the current foreign and domestic technical surveillance threat.

e. (U) Authorize disclosure of TSCM information to foreign countries or international organizations after coordination with the appropriate national level interagency committees.

f. (U) Disseminate information on the technical surveillance threat to appropriate Army activities, to include information on the detection of new technical surveillance monitoring systems.

g. (U) Coordinate with other DOD components to establish the frequency of periodic TSCM support.

h. (U) Develop cross servicing agreements with other military departments for the conduct of TSCM support and informing the Assistant Secretary of Defense (Comptroller), on request, of the number and locales for which cross servicing agreements have been implemented.

i. (U) Ensure Army standards for the selection and training of TSCM special

agents are in accord with those set forth in DOD Instruction 5240.5.

2-2. (U) Commander, U.S. Army Materiel Command (AMC)

(U) The Commander, U.S. Army Materiel Command, through the Deputy Chief of Staff for Intelligence (DCSI), AMC, and Commander, U.S. Army Intelligence Materiel Activity (IMA), in coordination with the U.S. Army TSCM Program Director and the 650th MI Group TSCM Program Manager, will—

a. (U) Develop, test, evaluate, modify, fabricate, procure, and provide TSCM equipment, develop related processes and techniques; and conduct limited research to support this effort.

b. (U) Maintain liaison with other U.S. Government agencies and commercial firms to identify TSCM equipment and techniques useful in the TSCM program.

c. (U) Operate the National Inventory Control Point and the National Maintenance Point for TSCM and associated specialized nonstandard equipment in accord with AR 381-143.

d. (U) Validate and consolidate worldwide Army TSCM equipment requirements.

e. (U) Provide centralized procurement and issue of all TSCM equipment required by the U.S. Army.

f. (U) Maintain records of U.S. Army TSCM equipment purchased.

g. (U) Maintain records of TSCM equipment by identity of the Intelligence Property Book (IPB) account to which TSCM equipment is issued.

h. (U) Issue Army procured and owned TSCM equipment only to Army IPB accounts authorized TSCM equipment in accord with DOD Instruction 5240.5.

2-3. (U) Commander, U.S. Army Intelligence and Security Command (INSCOM)

(U) The Commander, U.S. Army Intelligence and Security Command, will—

a. (U) Establish and operate a centrally managed TSCM support program for the U.S. Army under the guidance and staff supervision of the ACSI, DA.

b. (U) Maintain a data base of Army facilities requiring periodic TSCM support, support rendered, and results of the support.

c. (U) Provide each MACOM a fiscal year listing of facilities validated for TSCM support.

d. (U) Establish procedures for the conduct and reporting of TSCM services of Army facilities as specified herein.

e. (U) Establish a TSCM special agent certification program as executive agent for the Army, to include selection and training of candidates, and maintaining certification records reflecting current and inactive TSCM special agents.

f. (U) Conduct TSCM support in accord with the general guidance published by Director, Central Intelligence (DCI) Procedural Guide No. 1, "Requirements for Reporting and Testing Technical Surveillance Penetrations;" in DCI Procedural Guide No. 2, "Requirements for Reporting and Testing Hazards;" and in DCI Procedural Guide No. 3, "Guidance for Conducting Audio Countermeasures Surveys."

g. (U) Appoint the U.S. Army TSCM Program Director.

h. (U) Carry out Army obligations assigned by the Tri Service TSCM Memorandum of Understanding.

i. (U) Authorize and encourage direct communication for the purpose of operations and logistics between the INSCOM TSCM Program Director, TSCM Program Managers, and Heads of TSCM Support Elements.

2-4. (U) Major Army commands (MACOMs) and Army agencies

(U) Major Army commands and separate Army agencies will—

a. (U) Limit the number of sensitive areas to the minimum consistent with operational requirements.

b. (U) Limit the amount of communications equipment and associated wiring in sensitive areas to that which is essential for operational requirements.

c. (U) Establish and maintain physical technical security measures for sensitive areas in accord with the minimum standards for security established in this regulation.

d. (U) Promptly notify the Army TSCM Program Director so that TSCM support may be rescheduled or cancelled when—

(1) (U) Any sensitive area is activated or closed.

(2) (U) Unexpected delays or activities such as military exercises, delays in construction requirements, or equipment installations occur.

(3) (U) Foreign nationals are working within or visiting the facility.

e. (U) Ensure prompt notification is made to INSCOM or the supporting TSCM element when TSCM support is scheduled but cannot be conducted due to unexpected delays or activities such as military exercises, delays in construction requirements, equipment installation, or foreign nationals working within or visiting the facility.

f. (U) Ensure that—

(1) (U) The security integrity of the area is maintained after receiving TSCM support.

(2) (U) Access to the sensitive area is limited to authorized and properly cleared personnel.

(3) (U) Continuous escort is maintained over all uncleared personnel.

g. (U) Indoctrinate personnel on—

(1) (U) The threat posed by the employment of technical surveillance devices.

(2) (U) The requirements for reporting suspect devices or activities.

h. (U) Take prompt action to eliminate technical and physical security deficiencies and vulnerabilities identified as a result of a TSCM service.

i. (U) Limit knowledge of pending TSCM services to personnel with a specific "need-to-know," maintain routine operations prior to and during conduct of the TSCM support, and prohibit discussions of the pending support within the sensitive area.

j. (U) Thoroughly inspect furnishings and equipment introduced into sensitive areas and ensure these items are inspected only by the most qualified security and/or technical maintenance personnel available.

k. (U) Ensure that the TSCM team is not unduly delayed and has unrestricted access in the area to be serviced.

2-5. (U) Army intelligence components

(U) Commanders of Army intelligence components or activities will ensure—

a. (U) Operational security is maintained for TSCM requirements.

b. (U) TSCM services are performed only by teams meeting certification requirements established in this regulation.

c. (U) TSCM special agent personnel attend scheduled refresher and advanced training.

d. (U) TSCM special agents assigned to authorized TSCM positions are used in the primary mission of TSCM duties.

e. (U) TSCM certificates issued to Technical Surveillance Countermeasures special agents (TSA) and Master Technical Surveillance Countermeasures special agents (MTSA), are returned to the INSCOM TSCM Program Director in the following instances:

(1) (U) Assignment of a TSCM special agent to a non-TSCM validated position.

(2) (U) Removal of additional skill identifier (ASI) (9L or G9) or withdrawal of military occupational specialty (MOS).

(3) (U) Removal from TSCM operations or non-utilization of TSCM skills for periods of 12 months or more.

(4) (U) Failure to participate in scheduled refresher training.

(5) (U) Retirement, release from active duty, or expiration of term of service.

Section II
(U) Policies (U)

2–6. (U) Standardization

(U) In compliance with DOD Instruction 5240.5, DA will standardize TSCM equipment, procedures, and reports as much as possible in order to increase the potential for cross servicing. In an effort to reduce expenditures and to eliminate duplication, DA will coordinate with the other military departments to achieve the most efficient cost effective program. INSCOM will establish cross servicing agreements with the other military departments to ensure that the military department having geographical responsibility for the area is tasked to conduct required TSCM support.

2–7. (U) Operations

a. (U) TSCM surveys, inspections, preconstruction technical services, technical advice or assistance, and related TSCM investigations will be conducted only by TSCM special agents assigned to authorized TSCM positions in the U.S. Army Intelligence and Security Command and the 650th Military Intelligence Group. Consistent with DCI Procedural Guides Numbers 1, 2, and 3, DOD Instruction 5240.5, AR 381–10, and AR 381–20, TSCM teams will be afforded maximum consideration for operational security. A TSA will wear civilian clothing and when on operational temporary duty (TDY) will not use Government dining facilities or quarters. Equipment having the capability of detecting technical surveillance devices will be acquired or possessed only by those organizations authorized to conduct validated TSCM services or investigations and will be operated only by TSCM special agents.

b. (U) At least two TSCM special agents are required to conduct an instrumented technical service and at least one team member must be a certified Technical Surveillance Countermeasures special agent (CTSA). A minimum of one TSCM team will be continuously assigned to a TSCM support element where TSCM equipment is authorized.

2–8. (U) Authorized TSCM support

(U) TSCM investigations and services authorized to be conducted by U.S. Army TSCM special agents are—

a. (U) TSCM survey.

b. (U) TSCM inspection.

c. (U) Preconstruction technical advice and assistance.

d. (U) Technical penetration/hazard investigations.

2–9. (U) Other TSCM support

(U) TSCM support will be provided as follows:

a. (U) *Direct special support.* Activities of certain high level DA and DOD authorities or organizations are considerated to be of such sensitivity as to warrant special TSCM support. These requirements will be identified by the ACSI, DA, and validated by INSCOM for appropriate TSCM support.

b. (U) *Validated services.* Facilities will not automatically qualify for recurrent TSCM support. Recurrent support to a facility and the frequency of approved periodic services will be determined by the TSCM Program Director based upon a documented threat and an assessment of the vulnerability of the facility with specific consideration given, but not limited to, the following:

(1) (U) Known or suspected hostile intelligence activities within the geographical area of the facility.

(2) (U) Security measures, or lack thereof, in effect at the facility.

(3) (U) Sensitivity of information susceptible to technical penetration.

c. (U) *TSCM cross service support.* A TSCM support will be provided by the Army to the facilities or activities of other military departments in accord with established cross servicing agreements on a nonreimbursable basis. The frequency of periodic TSCM support to cross service facilities will be as determined by each military department in accord with guidance contained in DOD Instruction 5240.5 and as reflected in service regulations of the individual military departments.

2–10. (U) Requests for TSCM support

(U) Requests for TSCM support to Army facilities or activities will be submitted to INSCOM for sensitive areas only. These requests will be submitted through MACOM's or separate Army agencies. Such requests are subject to the procedures and validation criteria in chapter 3. TSCM service is not an end in itself and imposes certain requirements on the requestor. Due to the limited availability of TSCM equipment and personnel resources, a high degree of selectivity must be exercised by requestors in identifying areas to be supported.

2–11. (U) Reporting possible technical surveillance penetrations

(U) A suspected technical surveillance penetration, or the discovery of a technical surveillance device, as defined in the glossary of this regulation, in any facility, regardless of the facility's relative sensitivity or apparent unclassified nature, will immediately be reported in accord with chapter 5.

2–12. (U) Public disclosure of TSCM activities

(U) The public disclosure of information relating to TSCM activities, equipment, or technical surveillance devices or techniques (method of operation), which could adversely affect the TSCM program or the U.S. Army will be authorized only by ACSI, DA. Requests for records under the Freedom of Information Act will be processed in accord with AR 340-17.

2–13. (U) Foreign disclosure

(U) The release of information relative to technical surveillance penetrations and hazards, TSCM equipment, TSCM serviced areas or schedules of TSCM services, and technical security equipment to foreign nations or any international organization will be authorized only by the ACSI, DA, after coordination with the appropriate national level committee.

2–14. (U) In-place monitoring systems (IPMS)

(U) Highly sensitive projects or facilities may augment their TSCM support by use of IPMS. Equipment purchase, installation, and operation will be funded by the organization using the system. IPMS or IPMS equipment will not be purchased or operated without the prior coordination and approval of the INSCOM TSCM Program Director. Any technical penetrations or hazards discovered with the use of IPMS equipment will be reported in accordance with paragraph 2–11.

2–15. (U) TSCM priorities

(U) Established priorities for TSCM activities and investigations are as follows:

a. (U) *Priority I.*

(1). (U) Technical surveillance penetrations or hazards.

(2) (U) Valid emergency technical support.

(3) (U) Preconstruction assistance.

b. (U) *Priority II.* Technical programmed support.

c. (U) *Priority III.* Technical unprogramed support.

Section III
(U) Selection and Training of TSCM Special Agent (TSA) Personnel (U)

2–16. (U) Minimum selection standards

a. (U) *Physical requirements for entry and retention.*

(1) (U) Hearing acuity test results per audiometer test not to exceed plus 15

decibels at frequencies of 250, 500, 1,000, 2,000, and 4,000 Hz.

(2) (U) Both eyes distant vision 20/20 and near vision J-1. Correction of vision through glasses to achieve these results is acceptable.

(3) (U) Color perception test results, employing the pseudoisochromatic plates for testing color perception, not to exceed four incorrect identifications out of 14 test plates.

(4) (U) Free from any physical defects which materially hinder manual dexterity.

b. (U) *Security clearance.* (U) TSCM special agents require access to TOP SECRET information and must be cleared for access to sensitive compartmented information (SCI).

c. (U) *Special qualifications for entry.*

(1) (U) *Warrant officers/commissioned officers.* Must be a CI technician (971A)/ CI officer (36A) and a member of the active Army with a minimum of 4 years', but not more than 16 years', active military duty.

(2) (U) *Enlisted personnel.* Must be a CI agent (97B) in grade E5 or above, have favorably completed the probationary period for retention of the 97B MOS, and a member of the active Army with a minimum of 4 years, 'but not more than 16 years', active military duty.

d. (U) *Education.* Completion of high school or equivalent. Must have credit for high school level algebra or have a standard score of 120 or higher in the electronics (EL) aptitude area.

2-17. (U) Application procedures

a. (U) Application for training and entry to the TSCM program will be submitted on DA Form 4187 (Personnel Action) in accord with DA Pamphlet 600-8, procedure 3-10, to DA MILPERCEN ATTN: DAPC-EPL-M. Applicant must have a current (5-year) special background investigation (SBI), or action must have been initiated for a SBI at the time of application. In the latter case, final selection will be conditional upon completion of a favorable SBI.

b. (U) Prior to acceptance for formal TSCM training, the applicant will be interviewed by a CTSA or MTSA assigned to an authorized TSCM position.

c. (U) Prior to acceptance for formal training, applicants will voluntarily acknowledge a 3-year utilization obligation to commence upon successful completion of the TSCM course.

2-18. (U) Mandatory and desirable training

a. (U) The following courses are mandatory training subjects for all TSAs:

(1) (U) Technical surveillance countermeasures techniques.

(2) (U) Telephone systems and equipment.

(3) (U) Protective systems to include intrusion detection systems, security devices and equipment, and physical security construction requirements.

(4) (U) Signal identification.

b. (U) The following courses are desirable training—

(1) (U) Advanced signal identification.

(2) (U) Advanced antenna design and use.

(3) (U) Optical systems as pertain to technical penetration and advanced communications.

(4) (U) Computers and digital logic principles and applications in relation to TSCM and technical penetrations.

2-19. (U) Certification of TSCM special agents.

a. (U) TSA candidates will complete certification requirements in accord with criteria established by the Army TSCM Program Director, to retain the TSCM ASI and remain the TSCM program.

b. (U) Noncertified TSAs will work under the direct supervision of a CTSA or MTSA.

c. (U) TSCM positions will be filled by TSAs. CTSAs not assigned to a valid TSCM position will not maintain active certification and are not authorized to maintain a certificate. TSAs will attend scheduled refresher/update training to retain certification and maintain proficiency.

2-20. (U) Awarding/Withdrawal of ASI

a. (U) The ASI will be awarded upon successful completion of the prescribed course of instruction as follows—

(1) (U) Award ASI 9L for warrant officers.

(2) (U) Award ASI G9 for enlisted personnel.

b. (U) Recommendations for removal of ASIs may be made to the Commander, MILPERCEN by the INSCOM TSCM Program Director in the following instances:

(1) (U) Upon sufficient written justification to the INSCOM TSCM Program Director that it is in the best interests of the Army that the ASI be withdrawn.

(2) (U) Upon recommendation by the INSCOM Certification Board for one of the following:

(a) (U) Nonutilization of TSCM skills for a period of 3 years or more.

(b) (U) Assignment to a position that does not require use of instrumented or operational TSCM skills for a period of more then 3 years.

(c) (U) Failure or refusal to attend scheduled TSCM refresher training.

(d) (U) Failure to complete INSCOM TSCM certification requirements.

(e) (U) Failure to maintain minimum physical selection standards as outlined in paragraph 2-16a and security clearance standards outlined in paragraph 2-16b.

Chapter 3
(S) TSCM Request and Reporting Procedures (U)

Section I
(S) Requests (U)

3-1. (U) General

(U) TSCM services (surveys, inspections, and preconstruction activities and technical penetration investigations) are highly specialized counterintelligence investigations and are not to be confused with compliance oriented or administrative services conducted to determine facilities' implementation of various security directives. Correction of identified vulnerabilities will only enhance the security posture of sensitive areas and all TSCM special agents are obligated to work closely with commanders and facility representatives to ensure sensitive areas are devoid of technical surveillance devices, technical security hazards, and physical security weaknesses. Application of physical and technical control measures, and the evaluation of their effectiveness through the TSCM survey and inspection program represent a considerable investment in highly technical manpower resources and dollars.

3-2. (U) Scheduling of TSCM support

(U) TSCM support of sensitive facilities will be validated by the INSCOM TSCM Program Director and scheduled based upon criteria set forth in paragraph 2-9b. Army activities will comply with the responsibilities of paragraph 2-4d, to avoid INSCOM validating and scheduling unnecessary services.

3-3. (U) Requesting TSCM support

a. (U) Requests for TSCM support to Army activities in accord with paragraph 2-9 will be considered on a case-by-case basis and should be forwarded through the MACOM to Commander, INSCOM, ATTN: IAOPS-CI-TC, Arlington Hall Station, Arlington, VA 22212-5000. Fully justified requests of an emergency nature, or for new facilities, may be submitted at any time, but should be submitted at least 90 days prior to the date the support is required. Unprogrammed services will be funded by the requestor. Each request for unprogrammed TSCM support must be accompanied by a fund cite to defray the costs of TDY and per diem.

nance points do not qualify for TSCM support.

(5) (U) TSCM support will not be provided for TEMPEST-identified or related problems or for suspected emanations from sensitive information-processing equipment unless it is suspected that emanations are caused by unauthorized modifications made to the equipment or area to intentionally cause such emanations.

b. (U) In addition to the above criteria, one or more of the following criteria must apply:

(1) (U) The area is subject to support under the provisions of paragraph 2-9a, b, or c.

(2) (U) Construction has been accomplished within the area by uncleared, unescorted personnel.

(3) (U) The area has been subjected to uncontrolled access by uncleared personnel due to emergency (fire, natural disaster, mob actions, etc.)

(4) (U) The area has been accessed by a known or suspected defector or hostile intelligence agent.

(5) (U) The area is a newly designated or constructed facility and requires an initial survey.

3-9. (U) Tasking

a. (U) INSCOM will task the appropriate field operating activity, or other military department under cross servicing agreements, to perform the necessary services for all validated TSCM support requirements.

b. (U) In most cases, Army TSCM teams will provide the support; however, because of cross servicing agreements, a U.S. Navy or U.S. Air Force TSCM team may provide the support.

3-10. (U) Conducting TSCM services

a. (U) TSCM services will be conducted using procedures outlined in DCI Procedural Guide No. 3. Minor variations required to fill unique customer or facility requirements are permitted.

b. (U) Occupants of the area will be instructed not to make comments that would serve as an indicator to an agent conducting a technical penetration that a TSCM service is to be conducted or is in progress. Such comments or statements will be treated as security violations and the TSCM team chief will—

(1) (U) Stop all activity and evaluate the situation and, if the evaluation indicates a compromise has taken place, notify the appropriate Field TSCM Program Manager.

(2) (U) If directed by the Field TSCM Program Manager to terminate the support, inform the security manager responsible for the area—

(a) Of the nature of the incident

(b) (U) That the support has been terminated due to compromise

(c) (U) That the compromise under this regulation will be treated as a security violation.

(3) (U) Provide information regarding the incident, actions taken, evaluation of the cause, and impact on future support to the facility under the comments paragraph of the Counterintelligence Technical Service Report.

3-11. (U) Exit briefing

(U) An exit briefing will be conducted at the conclusion of all TSCM services and all findings and recommendations will be made known and discussed with appropriate officials. TSCM teams will inform the officials that findings and recommendations will not be considered official until they have been evaluated and the report signed by the authorizing official of the agency or unit conducting the service. The commander of the inspected facility should be present during the exit briefing. If the commander is not available, an authorized facility representative will be present.

3-12. (U) Action after TSCM service

a. (U) The facility commander will evaluate all technical security deficiencies or hazards and physical security weaknesses identified in the TSCM report and take action to correct the identified vulnerabilities.

b. (U) The facility commander or responsible security official will ensure procedures exist to prevent compromise of the secure status of the sensitive area, such as—

(1) (U) Admission of unauthorized or uncleared persons unless continuously escorted by personnel familiar with the security requirements of the area.

(2) (U) Failure to maintain continuous and effective surveillance and control of the area.

(3) (U) Repairs or alterations to or within the area without the supervision of qualified personnel.

(4) (U) Introduction of new furnishings or equipment which have not been thoroughly inspected by qualified security or maintenance personnel.

Section II
(U) TSCM Reports (U)

3-13. (U) Format

(U) Reports will be prepared for all TSCM services in letter form, with annexes or enclosures, as required.

3-14. (U) Classification

(U) Classification of TSCM related information, correspondence, summaries, or activities, is as follows:

a. (U) Correspondence or documentation that identifies facilities receiving or pending TSCM support, or identified as a TSCM target, will be classified at least SECRET with OADR for declassification. The classification will apply so long as the facility is identified as a recipient of recurring TSCM services.

b. (U) Technical summaries and correspondence pertaining to major security vulnerabilities, at a minimum, will be classified SECRET, OADR for declassification instructions. Minor security vulnerabilities normally will be classified CONFIDENTIAL, OADR, and annotated with instructions preventing release to foreign nationals.

c. (U) Information that refers to the discovery or alleged discovery of a technical surveillance device or technical penetration, as defined in the glossary, will be classified, as a minimum, SECRET, OADR.

d. (U) Information that reveals the capabilities or limitations of TSCM equipment, TSCM equipment budgets, or TSCM procurement actions, will be classified up to SECRET, declassified OADR.

e. (U) Classification authority will be cited as CLASSIFIED BY: Para E7, DOD Instruction 5240.5, dated 23 May 84, OADR.

3-15. (U) Report content

a. (U) TSCM surveys, inspections, and preconstruction reports will reflect only those insecure conditions which could permit the transmittal of sensitive information to unauthorized persons through technical or physical penetration of the facility, or technical security hazards. References are cited to provide additional clarification to the requesting authority.

b. (U) Reports of TSCM services will contain the following information:

(1) (U) Servicing agency.

(2) (U) INSCOM FY sequence number.

(3) (U) Type of service.

(4) (U) Full identification of the supported facility (COMSEC account number will be included for AR 380-40 support).

(5) (U) Inclusive dates of support.

(6) (U) Regulating authority for conducting the service and/or other specific directives which prescribe security standards.

(7) (U) Date and identity of agency or element providing the last TSCM service and the type of service provided.

(8) (U) A listing of accompanying enclosures.

(9) (U) A statement describing the sensitivity of the facility with regard to the level and frequency of classified information processed and discussed.

(10) (U) A narrative paragraph containing—

(a) (U) A synopsis of identified vulnerabilities, or lack thereof, to include those items which both enhance and detract from the overall facility technical or physical security posture.

(b) (U) An assessment of the facility's relative compliance with appropriate security regulations and directives.

(11) (U) Specific findings and recommendations. These will be attached as enclosures. Security weaknesses or vulnerabilities found during the service will be described in detail and the appropriate reference will be cited to provide additional clarification to the requesting authority. Findings for which there are no appropriate references will be included as noncitable. Recommendations to remedy identified security weaknesses or vulnerabilities will be stated in conjunction with each finding. Recommendations should be consistent with regulations, known exploitable technical or physical vulnerabilities, and knowledge of identified technical security hazards. Recommendations will be carefully evaluated in terms of implementation costs and, where practical, alternatives will be offered for elimination of exploitable technical or physical security vulnerabilities.

(12) (U) A statement acknowledging that all aspects of the TSCM service were discussed with the facility commander and/or his or her representative. The date of the exit briefing and full name, identity and position of facility officials present will be included. If an exit briefing was not conducted, the reason will be given.

Chapter 4
(U) Physical and Technical Security Standards (U)

Section I
(U) Introduction and Physical Security Standards (U)

4–1. (U) Introduction

(U) Upon the effective date of this regulation, compliance with these standards is mandatory for all facilities or areas requiring TSCM services. Existing, previously approved, or serviced facilities need not be modified to conform with these standards; however, renovations or modifications planned or made to an existing facility will conform with the requirements of this regulation. There may be instances in which circumstances constitute a threat of such proportion that they can only be offset by stringent security arrangements over and above those prescribed herein. Conversely, there may be instances at which time, location, condition, or use of the facility, or other unforeseen factors may make full compliance with these standards unreasonable or impossible. These situations will be referred to the MACOM for consideration and possible deviation from prescribed standards. Requests for waivers to existing security standards will be made to the MACOM, will include complete justification, and will outline the protective measures taken by the facility to provide adequate protection in lieu of the waived requirement. The MACOM, on a yearly basis, will withdraw or reissue all waivers and review all waivers granted for changes or other factors which could nullify the original justification, i.e., change in mission, change in use of the facility, external factors, etc. Waiver will be an item of inspection for all services rendered and, if found to be inconsistent with good security practices or standards, recommendations will be made for their withdrawal.

4–2. (U) Perimeter security

(U) Sensitive areas must be constructed to provide a reasonable degree of protection against forced entry and a high degree of protection against surreptitious entry. The requirements for physical and acoustical security necessitate that all windows and doors of sensitive areas remain closed and secured at all times. By the nature of their construction, these areas cannot provide adequate ventilation, unless environmental controls are included during construction. Without environmental controls, high temperatures, humidity, and constant operation of electronic equipment can make working conditions unbearable.

a. (U) *Perimeter doors.*

(1) (U) A perimeter door should be a solid core 1¾ inch thick wooden door, a wooden door faced on the exterior side with 16 gauge sheet metal, or a commercial door of metal clad construction. The door must provide the same level of sound attenuation as that required for the perimeter walls. Sound attenuation requirements are outlined in paragraph 4–3a(4).

(2) (U) Perimeter doors will normally be mounted on interior hinges. Where it is necessary to use exterior hinges, action must be taken to prevent removal of the hinge pins as a method of gaining unauthorized access. Exterior hinges require that each hinge pin be welded to its respective hinge. As an additional option, substantial metal pins may be set into the edge of the door frame so the door cannot be opened even if the hinge pins are removed.

(3) (U) Each perimeter door will be equipped with a heavy duty pneumatic door closer.

(4) (U) Entrance doors opening into uncontrolled areas will be equipped with a wide angle peephole viewing device which permits one-way observation only.

b. (U) *Main entrance doors.*

(1) (U) Main entrance doors are perimeter doors used for regular entry and exit from the facility. To prevent unauthorized access during periods of occupancy, equip main entrance doors with mechanical or electronic access controls.

(2) (U) Main entrance doors will be equipped with one of the following type locking devices:

(a) (U) A Sargent and Greenleaf Model 8470 Group 1R combination lock assembly with a dead bolt. The lock must be equipped with a spy proof adjustable dial and ring, and a ½ inch thick drill resistant hardplate must be installed between the body of the lock and the interior side of the door. In addition to door hardware, the door locking bolt must interface with a heavy duty strike.

(b) (U) Main entrance doors serving VIP areas or areas not used specifically for the storage of classified information, may be secured with a locking system similar or superior to the security afforded by a locking system consisting of an Ultra 700 lock equipped with a Medeco cylinder using a 1½ inch throw bolt and heavy duty strike.

c. (U) *Vault doors.* Class 5 or 6 vault, doors, while authorized, do not usually provide proper sound attenuation. Further, vault doors will not be used as access control doors in high traffic areas. Extensive use of a vault door will eventually weaken the locking mechanism, causing a malfunction of the emergency escape device, and constitute a security and safety hazard. To preclude this situation, a secondary access control door, which meets the acoustical requirements, must be installed immediately inside the facility. The back access plate of vault doors which stand open in uncontrolled areas will be protected by a lead seal or other protective device designed to prevent undetected access to any components of the locking mechanism. The vault door will be temporarily fastened in the open position during periods of facility occupancy to prevent accidental closing and locking of the door. To prevent damage to the locking mechanism, the locking bolts should not be extended as a method of precluding accidental closing of the door.

d. (U) *Emergency exit doors.* Emergency exit doors are perimeter doors designed to be used only on an emergency basis. All doors not equipped as main entrance

doors are emergency doors and will be equipped as follows:

(1) (U) Emergency doors will have as a minimum one heavy duty dead bolt and strike which provides protection equal or superior to that afforded by the main entrance hardware.

(2) (U) Emergency exit doors, where required by local fire code, may be equipped with a commercially produced combination panic bar and alarm which affords security equal or superior to that afforded by main entrance door hardware.

(3) (U) Emergency doors will not be equipped with exterior hardware or opening aids.

e. (U) *Access controls.*

(1) (U) A mechanical, electronic cypher lock or a card access system may be used as an access control on the entrance door.

(2) (U) Mechanical, electronic cypher or card access locks are designed for access control and provide no degree of security against forced or surreptitious entry. When unoccupied, the door must be secured with the built-in Group 1R combination lock on the main door.

(3) (U) Electric strikes or bolts used in conjunction with access control systems will be of heavy duty construction.

(4) (U) Electronic systems will have only the exterior access device (combination key box or card slot) mounted on the exterior of the facility. Wiring will be routed from the external access device directly through the wall into the sensitive area so that the wires are not accessible outside the secure perimeter. All other wiring and hardware will be located within the sensitive area.

f. (U) *Windows.* Windows represent a significant threat to the security of a facility, providing both a physical and technical vulnerability.

(1) (U) In new construction, windows are not authorized.

(2) (U) Windows will be removed in areas being remodeled for use as a sensitive area. The resulting openings will be filled with material equal in strength and density to that of the existing wall.

(3) (U) In areas where windows must be retained for preservation of the structure's historical appearance or for other compelling reasons, the following steps will be taken:

(a) (U) The windows will be secured in the closed position to prevent opening from within or outside the facility.

(b) (U) The inside surface of the window will be opaqued with black or silver paint, which gives the appearance of a normal transparent window from a distance.

(c) (U) The inside of the window will have a layer of fiberglass insulation compressed against the glass by a sheet of ¾ inch plywood or equivalent material. The plywood will be cut to fit the window aperture, and fastened in place. The edge of the plywood will be caulked to form an airtight seal with the wall.

(d) (U) Barriers constructed of bars or security screens (9 to 11 gauge expanded steel) to provide a reasonable assurance against surreptitious entry will be installed on the interior or the exterior of the window when warranted. Typical situations warranting barriers are ground level facilities, facilities where the exterior can be easily accessed, or in high threat areas. Security barriers will be installed in such a manner that they cannot be removed from outside the facility.

(e) (U) Due to variations in sound attenuation, methods of installation, and proper utilization, drapes will not be substituted for the window treatment standards described above.

g. (U) *False ceilings.* If the facility has a false ceiling which provides a means for surreptitious entry, an alarm system must be installed above the false ceiling to protect the area. False ceilings will be equipped with sufficient access ports to facilitate inspection of the entire area above the false ceiling.

4-3. Acoustical security

a. (U) Areas utilized for sensitive discussions will have perimeter walls, floors, ceilings, and doors which provide sufficient sound attenuation to prevent normal conversations from being overheard in adjacent areas by the unaided ear. This degree of sound attenuation is equivalent to a minimum sound transmission class (STC) or coefficient of 45. Sound attenuation and acoustic requirements do not apply to those sensitive areas officially designated and clearly marked or posted as "Non-Discussion" areas; for example, communication facilities, crypto repair points, and classified storage or vault areas. Sensitive areas in which sound amplification equipment is employed will require structural sound attenuation equivalent to a STC of 50.

(1) (U) Sensitive areas with perimeter walls, etc., which are contiguous to areas frequented by uncleared personnel or where access is uncontrolled, must employ at least one approved addition to the required STC of 45 such as a noise masking or cover music system.

(2) (U) Sensitive areas located in overseas areas where foreign nationals have access to contiguous walls, electrical, heating, cooling, or telephone services, etc., will require in addition to the required STC of 45, an approved noise masking or cover music system.

(3) (U) Doors constructed to meet the physical security requirements of this regulation will not normally provide sufficient sound attenuation to meet an STC of 45. Where possible consideration should be given to constructing a small vestibule immediately inside the main access door. The second interior door (of standard construction) in conjunction with the associated dead air space, will provide the required STC of 45. As a minimum, perimeter doors require installation of neoprene gasketing around the edge of the door frame and the door to form an acoustic threshold when the door is closed.

b. (U) Pipes, ducts, and conduits pose a significant acoustical threat in that they can efficiently pick up and transmit room audio out of the sensitive areaa.

(1) (U) All ducts and vents breaching the perimeter of the facility will be equipped with a nonconducting section installed immediately inside the sensitive area where the duct breaches the perimeter. Ducts will be fitted with sound diffusers.

(2) (U) All pipes and conduits breaching the perimeter of the sensitive area will be equipped with nonconducting sections.

(3) (U) In the event a pipe or duct cannot be equipped with a nonconducting section, the pipe or duct should be wrapped completely with sound deadening material.

(4) (U) When COMSEC or TEMPEST regulations require that pipes or conduits passing through a wall have a visible air space around them for inspection purposes, clear panels forming an airtight seal with the wall and the pipe or conduit will be placed on both the exterior and the interior side of the wall. The clear panels will be constructed of lexan, lexguard, or plexiglass having a minimum thickness of ⅜ inch. The panels will be cut to conform to the pipe, etc., and will be sealed in place with clear silicone rubber forming an airtight seal with both the pipe and wall.

(5) (U) In addition to acoustical protection, (b above), all vents and ducts which enter or egress an area from uncontrolled zones having dimenions greater than 90 square inches, must be protected with all of the following:

(a) (U) A security barrier constructed of hardened steel bars, ½ inch in diameter, mounted 6 inches on center vertically and horizontally and welded at all intersections.

(b) (U) An alarm device, capacitance or volumetric.

(c) (U) A steel screen with a maximum of a ½ inch square mesh to make difficult the introduction of a clandestine listening device.

(d) (U) A hinged inspection port, interior to the area, large enough to permit an

inspection of the duct and the installed security devices.

c. (U) Due to the high cost of constructing walls to provide STC 45, careful attention must be paid to preclude cracks, small air holes and nonstandard construction offering "flanking paths" which bypass the barrier and significantly decrease the overall sound attenuation. Wall locations should be carefully chosen to take advantage of existing walls which extend from the true floor to the ceiling and meet the prescribed physical and acoustical security standards.

d. (U) If a facility is used only as a communications center or computer center, and has no added functions other than those normally associated with such activities (message preparation and handling, computer printouts, distribution, etc.) and there is no discussion of sensitive information in the facility, the acoustical security standards above, and technical security standards of paragraph 4–6 are not required.

e. (U) To preclude unnecessary expenditures, all construction designed to meet the requirements of this section should be initiated only upon receipt of the final report through command channels.

4–4. (U) Intrusion detection systems (IDS)

a. (U) *Purpose.* The purpose of an intrusion detection system is to detect an intrusion or attempted intrusion into a sensitive area and to notify appropriate response/guard force personnel.

b. (U) *Concept.* The requirement for an IDS is dependent on a number of variables. The physical location of the facility, number and type of guards, hours of operation, type of construction, and the degree of threat must all be considered when deciding if, and what type of an alarm system is to be used.

c. (U) *Factors.* The factors that determine whether or not a sensitive area must have an IDS system are –

(1) (U) Location

(a) (U) Within the United States.

(b) (U) Outside the United States.

(2) (U) Type of operation.

(a) (U) Continuous.

(b) (U) Noncontinuous.

(3) (U) Sensitivity of information.

d. (U) *Requirement for alarms.* If an alarm is required—

(1) (U) All perimeter doors will be equipped with high security balanced magnetic door switches.

(2) (U) Non-vault type doors will be completely covered with either alarm lacing, capacitance grid, or foil pad whenever the exterior of these doors face an uncontrolled area (e.g., an open area not secured, guarded, or controlled). However, this is not required if the facility is protected by a volumetric alarm system.

(3) (U) The interior of sensitive facilities including areas above false ceilings, will be protected with a volumetric alarm system.

(4) (U) All windows not protected with a physical barrier, will be alarmed to detect any attempts of unauthorized entry.

e. (U) *Volumetric alarm systems.* Volumetric alarm systems may not be required in the following circumstances:

(1) (U) The perimeter walls are protected with an acceptable perimeter alarm system, and the true floor and ceiling meet structural requirements.

(2) (U) Guards randomly patrol within or around a closed storage facility at least twice each hour.

(3) (U) When individual security containers in a closed storage facility are alarmed and the guard response time is 5 minutes or less.

f. (U) *Types of alarms.*

(1) (U) *Balanced magnetic switch.* Magnetic switch sensors are used to detect unauthorized opening of doors, windows, safes, vaults, file cabinets, hatches, fire doors, and similar entry ways.

(2) *Capacitance alarm.* A sensor which alarms at an intruder's touch or, in some instances, close proximity. It can be applied to safes, file cabinets, ducts, grill work, windows, doorknobs, and other objects requiring protection.

(3) (1) *Volumetric alarms.*

(a) (U) *Motion detection.* A sensor which alarms upon detecting motion in a protected area. This type can include microwave, ultrasonic, or infrared sensors.

(b) (U) *Vibration detection.* Consists of sensors mounted on walls, ceilings, floors, and/or doors. If penetration of the protected area is attempted utilizing drills, chisels, crowbars, saws, cutting wheels, hammers, or similar tools, the continuous vibrations or repeated sharp blows will activate an alarm. Provides protection against forcible entry but none against surreptitious entry which might not employ force.

g. *Classes of electronic line supervision.* Whenever these requirements specify an alarm system class, they are referring to the method of transmitting an alarm signal.

(1) (U) *Class A. Pseudo-random digital and tone-wire transmitted preferred.* (Exceeds previous "high line security" requirement).

(a) (U) These systems will transmit over wire a pseudo-random generated tone or tones or digital type modulation. These systems will use either an interrogation and reply scheme or a synchronization scheme. The signal between the protected premises and the monitor location must not repeat itself within a 6 month period. A line supervision alarm signal will cause a lock-in condition which will be transmitted to the monitor location in not more than 30 seconds.

(b) (U) It must not be possible to compromise a Class A system by the use of resistance, voltage, or current substitution techniques.

(2) (U) *Class B. Digital and tone-wire transmitted prefered.* (Formerly described as "high line security.")

(a) (U) The system using digital or tone type modulation over transmission lines must use an interrogation and reply scheme. The signaling technique used for the interrogation must be different than that of the reply. Each line supervision alarm signal will cause a lock-in condition whch will be transmitted to the monitor location in not more than 90 seconds.

(b) (U) It must not be possible to compromise a Class B system by the use of resistance, voltage, or current substitution techniques. The circuits and methods employed must be highly resistant to transmission line noise, such as cross talk, hum, transients, and the like.

(3) (U) *Class C. Alternating current (AC) and direct current (DC), wire transmitted.* (Formerly described as "standard line security.") The Class C circuit supervisor units must provide an alarm response in the monitor location in not more than 1 second as a result of any of the following changes in normal transmission line current:

(a) (U) Five percent or more in normal line signal when it consists of direct current from 0.5 milliamperes through 30 milliamperes.

(b) (U) Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5 milliamperes.

(c) (U) Five percent or more of any component or components in a complex signal upon which the security integrity of the system is dependent. This tolerance will be applied for frequencies up to 100 hertz (Hz). Component as used in this specification means AC or DC voltage or current, AC phase, or frequency duration.

(d) (U) Fifteen percent or more of any component or components in a complex signal upon which the security integrity of the system is dependent. This tolerance will be applicable for all frequencies above 100Hz. Component as used in this specification means an AC or DC voltage or current, AC phase, or frequency duration.

h. (U) *Specifications.* Pending revision of Interim Federal Specification, Alarm Systems Interior Security, only components meeting or exceeding requirements

listed in W-A-00450B (GSA-FSS) will be installed in sensitive areas. Installation of the Joint Service Interior Intrusion Detection System (JSIIDS) is authorized. When JSIIDS is employed, installation will be in accord with JSIIDS installation procedures when the data transmitter is not used. Advice on IDS systems can be obtained from the servicing TSCM element.

(1) (U) All of the volumetric alarm systems must be "fail safe" in respect to oscillator component failure. Component failure means that, if any component within the oscillator circuit fails, an alarm must be generated.

(2) (U) Vibration detection pickups are highly sensitive contact/audio microphones; therefore, in order to prevent audio from being transmitted outside the area, all vibration detectors must be interfaced using an alarm relay within the sensitive area to cut off or disconnect the sensors during periods the area is occupied.

(3) (U) Taut-wire and break-wire type alarm systems are not approved for installation within sensitive areas.

i. (U) *Alarm transmission line supervision.* If the entire alarm system, including annunciator panels which are monitored by response personnel, are contained inside of the protected area, no electronic line supervision other than constant direct-current need be employed. Radio frequency (RF) transmission links via free space or power lines between any alarm components are not authorized. If the annunciator panels and connecting transmission lines are not within the protected area, the transmission lines must have electronic line supervision as follows:

(1) (U) If the annunciator panel is located in the same building as the protected area, equip the alarm transmission lines with Class A or B line supervision. If the transmission lines are not equipped with Class A or B line supervision, then the transmission lines must be completely installed in electrical metallic tubing (EMT), or rigid conduit, and all joints epoxy-sealed. Line transmission must be a minimum of Class C.

(2) (U) If the annunciator panel and protected area are not in the same building, or if the transmission lines in example *h*(1) above are not in EMT or other rigid conduit, line supervision must be a minimum of Class B.

j. (U) *Control location.* Under no conditions will either the control unit or day-night (secure/access) switch be outside the protected area. The only components of any system that can be outside the protected area are the transmission lines between control unit and annunciator panel and the annunciator panel itself. The annunciator panel must be observed and safeguarded on a continuous basis.

k. (U) *Remote test.* All alarm detection equipment capable of being electrically remote tested must be so equipped. Such remote test equipment must, through overt violation of the alarm system, create an alarm condition within the area which the alarm system is protecting. The violation must occur at the detection device which is farthest away, electrically, from its master control unit.

l. (U) *Tamper protection.* All alarm devices and control units will be equipped with tamper switches. These switches will remain in the supervised loop at all times, regardless of whether the system is in the secure or access mode.

m. (U) *Power.* All alarm systems will be equipped with standby power.

(1) (U) Protected area alarm components will be equipped with a minimum of 24 hours of standby power.

(2) (U) The annunciator panel will be equipped with at least one of the following:

(a) (U) Twenty-four hours of standby power.

(b) (U) An emergency power generator or sufficient battery power to allow an uninterrupted switchover or a no-break emergency power system.

(c) (U) Adequate standby power to allow a response force to secure the area and provide security equal to or greater than that of the alarm system.

n. (U) *Control zones.* In large installations, sufficient separate zone control panels should be installed to pinpoint the area violated and eliminate confusion on the part of the responding forces. For example, in a large building, the various perimeter doors should be on separate zones so a response force can go immediately to the point of attempted entry.

o. (U) *Audible alarms.*

(1) (U) An audible alarm inside the protected area is not authorized except in the case where the annunciator panel itself is also inside the protected area. An audible alarm inside the protected area would alert an intruder that he or she has activated an alarm.

(2) (U) The response force must be capable of regularly arriving at the protected area within 5 minutes after an alarm is announced. Actual response time is determined by the number of minutes required for the response force to be physically present at the protected area once the alarm has been sounded at the annunciator panel.

p. *Testing and maintenance of alarm systems.* All alarm systems must be adjusted and maintained at the highest attainable sensitivity or tolerance to provide optimum performance. Sensitivity will be determined from the manufacturer's stated specifications and by testing the equipment upon installation. Facility representatives are responsible for conducting monthly tests of the system. A record of the tests will be maintained and will reflect the date of the test, the name of the person completing the test, results of the test, and any action taken in the event of malfunctions. Sample test procedures for minimum acceptable sensitivities are as follows:

(1) (U) *Motion detection.* Overt body motion (walking through the protected area at the rate of one step per second for 4 seconds) in areas protected by ultrasonics, microwave, and other motion detection devices.

(2) (U) *Balanced magnetic switches.* Actual opening of doors, windows or other openings which are protected by balanced magnetic switches.

(3) (U) *Capacitance alarm.* Attempts to—

(a) (U) Penetrate a system by extending hands, arms, or legs through the protected area (air ducts or vents).

(b) (U) Touch an item being protected (door, window, wall, etc.).

(c) (U) Move protected objects (security containers).

(4) (U) *Vibration detection.* Hammering with a 1 pound hammer or weight on walls, floors, or ceilings protected by vibration detection equipment. Preferably this should be done midway between detectors. Damage to surfaces finished with wall boards, plaster, wood paneling, etc., which are considered fragile surfaces, may be avoided by placing a piece of heavy scrap wood, about two feet long, against the point where the blows are struck. Three to six blows should cause an alarm.

(5) (U) *Other.* Alarm systems consisting of either lacing or foil pad will be tested only by qualified alarm technicians with appropriate electronic equipment. Alarm equipment which is used and thus tested daily (i.e., balanced magnetic switches) needs no monthly testing.

(6) (U) *Unannounced facility openings.* In addition to the above, periodic unannounced openings of a facility should be performed to test alarm responses by the monitoring guard force. These exercises should be used to determine the actual alarm response time and the ability of the guard to implement alerting procedures associated with alarm annunciations during security hours. The test should be conducted in the spirit of assisting the guards in improving their performance, thus increasing the security provided the facility, but should not be so frequent as to be considered a nuisance to guard personnel. Testing will be coordinated with

guard personnel who monitor the alarm systems.

(7) (U) *Monthly power systems tests.* Power systems will be tested monthly and a record will be maintained of each test.

q. (U) *Computer controlled IDS for use within sensitive areas.* These will require the prior approval of the IMA, before installation. The requestor will provide as a minimum the following information:

(1) (U) Name and manufacturer of IDS.

(2) (U) Number of alarm zones being used and equipment in each zone.

(3) (U) Type of line supervision and computer's interrogation rate.

(4) (U) Location of monitor station.

(5) (U) Additional uses of the computer (i.e., access control, fire alarm energy monitoring, etc.). IMA will provide any additional requirements for approval of requested alarm system.

r. (U) *Access control.* An entry-control system functions in a total physical protection system to allow movement of authorized personnel and material through normal access routes and to detect and delay any unauthorized movement.

(1) (U) *Types of entry-control systems.*

(a) (U) *Manual system.* Employs personnel or a guard force to control access (includes machine-aided manual system).

(b) (U) *Automated system.* Allows personnel to enter and exit without guard intervention unless an alarm occurs.

(2) (U) *Approval.* Prior approval from IMA will be obtained before procurement of this type of system. As a minimum the following data must be provided:

(a) (U) Name of manufacturer.

(b) (U) Complete identification of unit, model, etc.

(c) (U) Number of readers and locations.

s. (U) *Closed-circuit television (CCTV).* CCTV systems can be helpful in augmenting a guard force by providing for surveillance, or verification of an alarm condition, for doors, hallways, fences, roofs, and similar avenues of approach or entry. Cameras should be repositioned weekly to prevent presentation ("burning") of a constant image on the monitor. If a CCTV camera is installed as a protective device and viewing of the monitoring screen would reveal classified information, the system must be installed in accord with NACSIM 5203 and TB 380-7. Only CCTV systems employing video baseband signals are permissible. IMA approval must be obtained prior to acquiring a video alarm system.

Section II (U)
(U) Technical Security Standards (U)

4-5. (U) Electronic equipment

a. (U) *Personally owned equipment.* Personally owned receiving, transmitting, recording, amplification, and processing equipment such as telephones, radios, tape recorders, televisions, video tape players or recorders, stereos, computers, etc., are not permitted within the controlled space of a sensitive facility under any circumstances. The introduction of calculators into secure areas must be controlled. As a general rule, these devices should not be restricted from a facility as long as they are in the personal possession of cleared personnel. Personnel using this equipment within the facility must be aware that they are ideal hiding places for clandestine listening devices, and that once inspected and introduced into the facility they should remain within the facility. Additional guidance regarding the use of computers is outlined in AR 380-380.

b. (U) *Government owned equipment.*

(1) (U) Government owned receiving, transmitting, recording and amplification equipment (for example: radios, music systems, tape and video recorders, television monitors (standard broadcast or closed circuit), television cameras, and amplifiers) must be declared mission essential by the local commander and authorized in writing by the facility chief or a responsible official prior to admittance in any secure facility. The authorization will identify the item by make, model, and serial number, and will include the mission essential justification for the introduction or utilization within the secure facility.

(2) (U) Government owned equipment introduced into the facility will be considered as RED or BLACK equipment, as appropriate, and is subject to the installation standards of TB 380-7 and NACSIM 5203. The items will be subjected to technical tests for clandestine surveillance devices and technical security hazards during the conduct of TSCM services.

(3) (U) Commercially designed equipment, unless properly shielded, will not be operated during classified discussions or activities. Further, the equipment must be disconnected from the power source and the antenna system.

4-6. (U) Telephone instruments and associated items

a. (U) *Concept.* The installation of telephones in sensitive areas is discouraged. Telephones present an unacceptable threat unless particular attention is paid to applying effective countermeasures. Controls must be placed on all telephone lines, active or inactive, to maintain any degree of telephone security. Telephone instruments will be kept to the minimum number required to support the facility mission requirements. All auxiliary telephone equipment/instruments must be safeguarded at a level commensurate with the sensitivity of the area in which installed. Requests for information on Telephone Security Panel (TSP) (see note) approved devices, or information on new devices proposed for TSP approval, may be submitted to the TSCM Program Director, INSCOM.

Note.—The TSP is the Telephone Security Panel of the TSCM Subcommittee Technical Countermeasures Working Group (TCWG).

b. (U) *Protective measures*

(1) (U) All telephone cables and wires, including those used for IDSs, will enter the secure area through one opening, and will be placed under control at the interior face of the perimeter. Each conductor will be accurately accounted for from the point of entry. The accountability will identify, through labeling and log or journal entries, the current status of each conductor.

(2) (U) When secure facilities employ dedicated key telephone of computerized telephone systems, the system will be installed within the secure perimeter of the area it is servicing. No telephone instrument controlled by these systems will be located outside the secure facility.

c. (U) *Telephone equipment.* All telephone instruments and associated equipment will be of U.S. manufacture. In cases where U.S. manufactured equipment is not available, is not compatible with the existing telephone exchange, or the installation of such equipment would compromise the covert status of the facility, telephones meeting Category I requirements will be installed.

(1) (U) *Category I.* The preferred telephone service for sensitive areas in that it provides the highest level of telephone security when installed and used is as follows:

(a) (U) Any instrument equipped with a positive disconnect plug-and-jack (the plug is to be removed from the jack at the completion of each call). An audible alarm will be installed in conjunction with the plug-and-jack to warn the user when the telephone is left plugged in, and the handset is replaced in the cradle.

(b) (U) When multiline telephone service is required, a single line telephone instrument utilizing a plug-and-jack connected through a key strip.

(c) (U) The factory installed ringer must be either removed, or the ringer signal leads electrically disconnected and isolated or shorted.

(d) (U) Ringing is to be accomplished by a TSP approved signaling device.

(2) (U) *Category II.*

(a) (U) When plug-and-jack telephone installation is not practical, the use of telephone instruments meeting the TSP design standards prescribed in Appendix B apply.

a. (U) No station or wiring will be located outside of the secure area, and all wiring will be installed to permit visual observation of the complete wire runs.

b. (U) Intercom systems will not use established power lines or any radio frequency means as the transmission link between stations.

Chapter 5
(S) Technical Surveillance Penetration/Hazards (U)

5-1. (S) Discovery of penetration (U)

[redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. (U) *The installation or activity security manager will request an immediate investigation by the supporting counterintelligence unit and/or supporting TSCM element.*

(1) [redacted]

(2) [redacted]

[redacted]

(3) [redacted]

5-2. (S) Reporting penetrations and followup actions (U)

(U) Reports will be submitted and the following actions taken:

a. [redacted]

b. [redacted]

c. [redacted]

[redacted]

(1) (S) [redacted]

(2) (S) [redacted]

(3) (S) [redacted]

(4) [redacted]

(5) [redacted]

d. [redacted]

(1) (S) [redacted]

(2) (S) [redacted]

(3) [redacted]

5-3. (S) Reporting TSCM hazards. (U)

[redacted]

5-4. (S) Resolving equipment irregularities (U)

[redacted]

[redacted]

5-5. (S) TEMPEST related anomalies (U)

(S)

[redacted]

Appendix B
Telephone Security Panel (TSP) Approved Telephone Design Standards

B-1. The features and properties required in the TSP approved telephone sets are provided below:

a. The lineswitch will be a manually operated metallic contact switching device actuated by the handset condition (on-hook or off-hook).

b. Unless specifically excepted in this standard, all components of the telephone are isolated from both tip and ring of the line pair(s) by the lineswitch when the handset is on-hook.

c. The line switch opens the following leads when the handset is on-hook.

(1) Tip and ring of line pair (both pairs for 4 wire use).

(2) Transmitter leads to network.

(3) Receiver leads to network.

(4) Any relay coil leads leaving the telephone.

(5) All control leads.

d. The lineswitch shorts (less than one-tenth ohm shunt) the following leads when the handset is on-hook:

(1) Leads to the transmitter element.

(2) Leads to the receiver element.

e. When the handset is placed on-hook, the lineswitch contacts for tip and ring will open prior to any other contacts.

f. The handset weight will be at least 2.5 times the minimum weight needed to operate the lineswitch.

g. The lineswitch operation will not be subject to internal or external obstructions.

h. Any use of multiple lineswitch plungers will be redundant. Depressing any one alone will fully operate all the on-hook lineswitch functions.

B-2. Line hold features

a. The telephone will incorporate an intrinsic hold mechanism.

b. The hold mechanism will not be isolated from the line pair(s) by the lineswitch.

c. (U) When activated, the hold mechanism will accomplish the following functions:

(1) Place an appropriate resistance across the line pair.

(2) Illuminate a "hold" indicator lamp located on the front of the telephone set.

(3) Perform the operations cited in B-1*c*(1) through B-1*c*(3) and B-1*d*, above, for the lineswitch.

d. Once activated, the hold functions will continue to operate independently of the lineswitch condition.

e. There will be no timeout of the hold functions.

f. The functions cited in B-2*c*(3) will require manual action to deactivate. They will not require Central Office (CO) or Key Telephone Service (KTS) current or voltage to operate.

B-3. Ringer

a. The telephone will provide the option for the ringer to be connected either across tip and ring of the line pair or across a separate signaling pair. The ringer is not isolated from the lineswitch.

b. The ringer will be constructed in accord with a design which is to be provided by TSP.

B-4. Key telephone features

a. Pickup line pair and control lead contacts for each line will be open unless a specific key association with the line is in the depressed (down) condition.

b. Only one pickup key can be depressed at a time.

c. Placing the handset on-hook will automatically restore all pickup keys to the up condition thereby opening all line pair and control lead contacts.

d. The pickup keys are not isolated from the line pair by the lineswitch.

B-5. Miscellaneous technical requirements

a. Except as called for by the TSP ringer design, the telephone must not contain any loudspeakers.

b. The telephone must not contain any integral speakerphone functions.

c. The telephone must not produce radiation or conduct electomagnetic interference in excess of the limits set for Class IC communication-electronic equipment in MIL-STD-461A, 7 February 1969 or its successor documents.

d. The telephone, while on-hook, must not draw more than 10 nanoamperes DC loop or ground current from a 400 ohm, 100 volt source across the tip and ring terminals.

e. The telephone must not be capable of performing as a cordless telephone set.

f. The telephone must not be capable of performing as a video telephone set.

g. The telephone must not be capable of performing hands free answerback functions.

h. The telephone must not contain any voice or sound activated on-hook functions.

i. The telephone must be capable of operating with both two wire and four wire systems.

j. The telephone set must not contain a carbon microphone. Electret transmitter elements must be used.

k. The telephone must contain high voltage protection devices which will prevent voltages greater than 150 volts from reaching any other component parts of the telephone set. The protective devices must not be isolated from the pair(a) by the lineswitch.

l. The telephone will provide a visual indication if it is drawing more than 100 nanoamperes of current from the line pair(s) while on-hook. The current sensor must not be isolated from the line pair(s) by the lineswitch. The display system may draw additional current, not to exceed two milliamperes, from the line pair if the sensor has detected the necessary 100 nanoamperes. The sensor should not respond to the additional current drawn for the display, it is only to respond to the intrinsic current drawn by the telephone.

m. The telephone must be a completely analogue unit. There must be no digitalization of voice signals at the telephone set.

n. The telephone construction must permit effective and expeditious TSCI inspection.

B-6. Administrative requirements

a. The telephone must be Federal Communications Commission (FCC) registered for connection to the Public Switched Telephone Network (PSTN).

b. Complete documentation must be provided on all matters relating to TSP approval.

c. Complete engineering drawings (schematic and assembly drawings) and circuit description must be provided for the telephone.

d. X-ray pictures of the telephone must be provided.

e. The manufacturer must ensure that the U.S. Government has unimpeded access to company engineers for consultations and clarifications with respect to the design and construction of the telephone.

Appendix A
References

Section I
Required Publications

AR 340–17
Release of Information and Records from Army Field Files. (Cited in para 2–12.)

AR 380–5
Department of the Army Information Security Program Regulation. (Cited in paras 3–4 and 3–7.)

AR 380–40 (C)
Policy for Safeguarding and Controlling COMSEC Information (U). (Cited in para 3–15a).

AR 380–380
Automation Security. (Cited in para 4–5a.)

AR 381–10
US Army Intelligence Activities. (Cited in para 2–7.)

AR 381–20
US Army Counterintelligence (CI) Activities). (Cited in para 2–7.)

AR 381–143 (C)
Logistics Policies and Procedures. (Cited in para 2–2c.)

DA Pam 600–8
Military Personnel Management and Administrative Procedures. (Cited in para 2–17a.)

TB 380–7 (C)
TEMPEST (U). (Cited in para 4–4s and 4–5b(2).)

DOD INST 5240.5
DOD Technical Surveillance Countermeasures (TSCM) Survey Program. (Cited in paras 1–1, 2–1i, 2–2h, 2–6, 2–7, 2–9c, 3–7k, and 3–14e.)

NACSIM 5203 (C)
Guidelines for Facility Design and RED/BLACK Installation (U). (Cited in paras 4–4s and 4–5b(2).) (This regulation is issued by the National Security Agency, Fort Meade, MD 20755.)

Section II
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 15–6
Procedures for Investigating Officers and Boards of Officers.

AR 190–53
Interception of Wire and Oral Communications for Law Enforcement Purposes.

AR 340–21
The Army Privacy Program.

AR 360–5
Public Information.

AR 380–10 (C)
Department of the Army Policy for Disclosure of Military Information to Foreign Governments (U).

AR 380–53
Communication Security Monitoring.

AR 381–1
Control of Dissemination of Intelligence Information.

AR 381–12
Subversion and Espionage Directed Against US Army (SAEDA).

AR 381–47 (S)
US Army Offensive Counterintelligence Operations (Short Title: OFCO) (U).

AR 381–100 (S)
Army Human Intelligence (HUMINT) Collection (U).

AR 530–1
Operations Security (OPSEC).

AR 530–4 (S)
Control of Compromising Emanations (U).

AR 604–5
Personnel Security Program.

DIAM 50–3
Physical Security Standards for Sensitive Compartmented Information Facilities.

FM 19–30
Physical Security.

DCI Procedural Guide No. 1 (S)
Requirements for Reporting and Testing Technical Surveillance Penetrations (U).

DCI Procedural Guide No. 2 (S)
Requirements for Reporting and Testing Hazards (U).

DCI Procedural Guide No. 3 (S)
Guidance for Conducting Audio Countermeasures Surveys (U).

Section III
Referenced Forms

DA Form 4187
Personnel Action

Appendix D
Guidelines for Computerized Telephone Systems

Section I
Introduction

D–1. Introduction

a. The U.S. telephone industry distinguishes between two basic forms of computerized telephone systems (CTS). These are the computerized private branch exchanges (CPBX) and the computerized key telephone systems (CKTS).

b. Private branch exchanges operate, essentially, as private telephone sub-networks. They tie together an internal group of subscribers into an independent network and provide external connections to the universal network by means of trunk lines to a telephone company central office exchange. Computerized private branch exchanges use stored program computer technology to perform the necessary message-switching functions. The resident computer in the modern commercial CPBX has made it possible to incorporate a multitude of attractive features for diverse applications. There are many features which enhance the basic telephone service but the applications are not restricted to telephone service; modern CPBX systems provide data processing, word processing, energy consumption control, communications traffic analysis, and other services in addition to processing telephone calls. CPBX systems were introduced in the 1970s and there are a great number of manufacturers from many countries now producing them. The various CPBX manufacturers often use their own terminology when referring to their products: private branch exchange (PBX), private automatic branch exchange (PABX), CBX, and similar terms are common. To a large extent, different technologies and approaches are being used by the different companies, but they all achieve basically the same objectives.

c. The computerized key systems (also referred to, variously, as hybrid key systems, business communications systems, office communications systems, and by other similar terms), despite their name, cannot at all be regarded as being merely advanced forms of the conventional key telephone systems typified by the Western Electric 1A2. The CKTS employ computer controlled switching operations similar to those of the CPBX and for the most part can realistically be characterized as small scale CPBX. The industry distinction is based in no small part on marketing rather than technical considerations.

D–2. Definitions

a. *Approved isolator.* A device or assembly of devices which has been accepted as effective by the TSP as a means to isolate or disconnect, for security purposes, an on-hook station or CTS from wires which exit the physical control zone (PCZ).

b. *Carrier.* A circuit card cage or shelf which is set up as an apparatus mounting for the CTS circuit cards. The carrier is provided with edge connectors to receive the circuit cards and is equipped with all wiring and hardware required for housing and interconnecting the system circuit packs.

c. *Call detail recording (CDR).* A record maintained by the CTS, or by auxiliary equipment, of specified types of calls. Typically, a CDR system will record the CTS station identity, date, time of day, duration of call, called party number, and trunk group type. A CDR is also a Station Message Detail Recording (SMDR).

d. *Frame, wiring frame, cross-connect frame.* An array of terminal blocks used to accomplish the interconnections between separated components of the system. In general, these interconnections (e.g., between the central office trunks and the CTS switching network, or between the telephone sets and the switching network) involve arrangements which are unique to each individual installation and cannot be built into the CTS. Wiring frames are usually composed of 66-type or 88-type wiring blocks.

e. *Line.* The wires (or other transmission media) which connect the station equipment to the CTS.

f. *Module.* The cabinets which contain the complete switching equipment for a subnetwork of a CTS. Some CTS divide the internal telephone network into separate subnetworks organized around switching node points. Calls between subnetworks are carried on intermodule links or through a switching node hierarchy. Control of the subnetworks may be by processors resident in the modules or from a central, common-control processor. Any cabinet which contains equipment in support of more than one subnetwork is designated a common-control cabinet and not a module cabinet.

g. *Network.* A system of individual stations arranged (subject to service constraints superimposed on it and not inherent in the system) so that any station can communicate to any other station by means of temporary connections at central switching nodes.

h. *Off-hook.* A station or trunk is termed off-hook if it is being used to initiate or actively engage in communications either with the CTS itself or with another station or trunk by means of a link established by the CTS.

i. *On-hook.* When a station or trunk is not being used to initiate or actively engage in communications via the CTS, it is termed on-hook.

j. *Physical control zone.* A continuous space continuously protected against unauthorized access or intrusion.

k. *Remote diagnostic support (RDS).* A means for an off-premises facility to perform diagnostic, maintenance, and programming functions on the CTS via the trunk connections to an external network.

l. *Remote maintenance, administration, and traffic system (RMATS).* Same as RDS.

m. *Station Message Detail Recording (SMDR).* Same as CDR.

n. *Station, station equipment station set, subscriber station.* Any telephone, console, data terminal, or other component of the CTS network which is connected to a communications port of the CTS and which is used to communicate, via a temporary switched connection through the CTS, to another station or to a trunk for access to an external network.

o. *Trunk.* Any connection from any external network (e.g., central office access to the public switched network, private lines, and tie lines to another CTS) to a communications port circuit of the CTS which can be used to provide access for CTS station equipment, via the CTS switched network, to that external network.

p. *Type-accepted telephone.* Any telephone whose design and construction conforms to the design standards for Telephone Security Panel approved telephone sets.

D–3. On-hook Security

On-hook audio security may always be achieved for stations located outside a PCZ, whether or not the CTS is to be installed within the PCZ, by providing them with approved isolators or by using type approved telephones. With either of these measures in force, the CTS may be treated as if it were essentially a central office and therefore it need not be located in the PCZ unless concerns other than on-hook audio are to be addressed.

D–4. CTS Installation

For situations in which the CTS, the system wiring, and the stations to be protected are all located within the same PCZ, the inherent isolation offered by the CTS can be used to avoid having to install approved isolators for the stations. In order to qualify for this usage, the CTS installation must be strictly organized so that it complies with the minimum stand-

Appendix C
Obsolete Category II Telephone Instruments

The following is a list of Western Electric Company (WECO) telephone instruments identified as Category II telephones prior to publication of the Telephone Security Panel recognized security design standards. Effective with publication of this regulation, these instruments will be installed as prescribed for Category I or III instruments.

500ABMU	Single-line, rotary dial
502AB/ABM	Single-line, rotary dial*
502BMW	Single-line, rotary dial*
568HSMW	Five-line, rotary dail (2-wires/4-wire)
680AMW2	17-line, rotary dial (2-wire/4-wire)
681AMW3	29-line, rotary dial (2-wire/4-wire)
2502BMW	Single-line, touch-tone dial*
2504B	Single-line, touch-tone dial (2-wire)
2568HM	Five-line, touch-tone dial (2-wire/4-wire)
2684AMW1	17-line, touch-tone dial (2-wire/4-wire)
2685AMW1	29-line, touch-tone dial (2-wire/4-wire)
2714A	Two-line, touch-tone dail, Princess
3504BW or C	Single-line, touch-tone dial (4-wire)
3568HHMW	Five-line, touch-tone dial, illuminated dial (2-wire/4-wire), special automatic voice network (AUTOVON)
3568HTMW	Five-line, touch-tone dial (2-wire/4-wire), special AUTOVON
3640A	18-line, touch-tone dial, special AUTOVON
3641A	30-line, touch-tone dial, special AUTOVON

*Note.—Indicates special purpose instrument to be used only with data communications (DACOM) secure facsimile systems. Instrument's exclusion switch feature must be wired to short out the telephone network, providing "voice up/data down" operation.

ards provided in section II, below. This will ensure that no means is afforded for on-hook audio to be present on any trunks or other wires external to the PCZ. Most telephone installations of interest involve special security conditions and other telephone security considerations in addition to the fundamental problem of on-hook audio. Application of the supplementary measures provided in section III will enable the CTS to address these concerns; these measures are recommended wherever operationally and administratively feasible.

a. Station equipment supported by the CTS but located in a nonconterminous PCZ is not protected by the isolation provided by the CTS installation. This equipment must be protected with approved isolators or be type accepted telephones.

b. The CTS used must conform to established guidelines with respect to country of origin.

Section II
Minimum Standards for Using a CTS to Provide On-Hook Audio Protection for Station Equipment

D–5. Physical security measures

A single PCZ with appropriate physical security encompasses all of the areas of concern.

a. The CTS is located in the PCZ.

b. All cables, lines, intermediate wiring frames, and distributed CTS equipment modules (to include voice and data links) are contained within the PCZ unless they are specifically and only dedicated to trunks or station equipment located outside the PCZ.

c. All program media (tapes, disks, etc.) are provided positive physical protection against unauthorized alteration. A certifiably correct master program is always maintained under secure conditions to be available as a check of the operating program and as a means of removing possible or identified software security deficiencies. Some CTS may not use program storage media of the type that can be duplicated and stored separate from the CTS. Where this is the case, a CTS may qualify under these provisions only if the user has, at all times, the means of obtaining a complete computer "dump" of program memory (to include generic program) onto an external medium which externally verified against a certifiable master copy that is kept safeguarded and updated. The comparison of current memory against the certifiable master must be performed frequently.

D–6. System configuration

The system configuration must effectively isolate the station equipment from all lines which leave the secure PCZ.

a. Two separate dedicated wiring frames (or a set of wiring frames) are maintained inside the PCZ containing the CTS to support connections with facilities outside that PCZ. These are terminated "external" wiring frames (in this paragraph) to distinguish them from frames used to connect the CTS to equipment located within the PCZ.

(1) The first "external" frame is used to terminate all lines entering from outside PCZ (central office trunks, tie trunks, telephones, etc.), on the customer side of the telephone company's demarcation point or network interface. This first "external" frame may be a connecting block similar to the one used for the Universal Service Order Code (USOC) RJ21X registration interface. (In such a case, there would be a 25-pair cable connecting the RJ21X block serving as a registration interface to the RJ21X-type block being used as the first "external" frame.

(2) The cross-connects continuing on from first to second "external" frame would be separated, single-pair wire, connected to the conventional insulation-displacement cut-down terminals of the RJ21X-type block.) In any case, whether or not RJ21X-type blocks are used to constitute the first "external" frame, the cross-connects from first to second "external" frame must be separate, single pair wire, and only pairs currently needed to extend active service to the CTS can be connected at any time.

(3) The second of the "external" frames provides the connection to the CTS.

(4) The two "external" wiring frames are separated by at least 3 feet from each other and from all other wiring frames. No cross connections are permitted between internal and "external" frames. The internal frames provide connections between CTS and peripheral devices such as telephones. They may be composed of "quick-connect" blocks with ready-manufactured patch cords (in lieu of the more conventional insulation-displacement cut-down blocks such as 66-type) if these blocks are not configured in such a way as to afford concealment for unauthorized cross-connects.

(5) CTS port circuit packs connected to "external" wiring frames are not installed in the same circuit carriers as those connected to internal frames and no two carriers share common cabling to the wiring frames.

(a) If a CTS cannot by itself qualify as an isolation device solely because it does not comply with these requirements (see note). This deficiency could be corrected by installing an approved isolator on every incoming trunk pair.

Note.—Either the configuration of its wiring frame, or frames, or the system configuration may not lend itself to separation of trunk-type cards and station-type cards in different carriers.

(b) The isolators must be located inside the PCZ, between the telephone company's demarcation point (network interface) and the system's wiring frames.

(c) At present, this alternative would preclude any station equipment outside the confines of the PCZ and, in fact, exclude any types of wires from entering the PCZ other than loop-start central office/PBX trunks. No isolators currently approved are capable of anything but loop start operation.

b. Each individual subscriber station has dedicated running wires to a specific, individual, port circuit of the CTS. Off-hook connections between port circuits are accomplished by metallic (or electronic) switching or by multiplex bus methods. The CTS keeps the running wires of every port circuit separate and unconnected from those of every other port except in the case of metallic switching, and then connections may only occur for ports actually engaged in an information interchange between off-hook subscriber stations (or between a station and a trunk). Audio coupling in either direction through a switch or between a port circuit and a multiplex bus only occurs when the associated station equipment or trunk is off-hook.

c. All telephones must satisfy the following on-hook requirements by means internal to the telephone (not dependent upon the CTS or subject to negation either by the CTS or by anyone with access to the mounting cord wires):

(1) No power is applied to any microphones.

(2) No power is applied to any audio circuits except as needed for incoming signaling.

(3) Receiver elements and speakers are shorted and/or provided with 60dB or more audio isolation from the mounting cord wires except during and as needed for incoming signaling. The 60dB minimum isolation applies only to signals from the receiver element (or speaker) to the mounting cord and not to signals arriving at the telephone from the mounting cord.

d. No port circuits or assigned station directory numbers are shared by extension stations inside the PCZ and extensions outside the PCZ. The extensions from the same port circuit or with the same station directory number are either all contained within the PCZ or all excluded from it.

e. Speakerphones are not permitted.

D–7. Prohibited functions

Some operational features that may be available with the CTS involve functions which are not consistent with good audio

security practices. These functions are expressly prohibited and any CTS feature employing them must be disabled.

a. The CTS must not be able to place or hold any subscriber station in an off-hook condition, or activate any function which should be off when the station is on-hook, unless directed to do so by that subscriber station itself. The off-hook condition is completely controlled by the station equipment.

b. There is no means for remote access to any CTS service.

c. Incoming calls (trunk and local) come to a console or telephone and are answered manually. There is no voice-activated pickup, automatic pickup (e.g., by telephone answering units and ADP terminals), or other responses of any kind to incoming calls except annunciation (initiated by the CTS) to the called station.

D-8. Administrative security measures

Administrative procedures are needed to ensure that none of the protective measures is intentionally or inadvertently degraded as a result of hardware or software changes to the system. Some of the administrative procedures are described functionally as requirements to be achieved. Their implementation may be any combination of physical security, systems configuration (hardware, software, and layout), personnel security, and technical countermeasures appropriate to the particular CTS and installation in question.

a. An appropriate minimum level of security clearance is determined by the cognizant agency for personnel having access for any purpose (to include installation and maintenance) to the station equipment, CTS components, wiring, and distribution frames located within the PCZ. Persons not possessing the minimum clearance will not be permitted access to the system except outside the PCZ or under suitable administrative safeguards. Merely providing an escort is not a safeguard against the system security being degraded unless that escort is technically competent and equipped to precisely monitor the work being done with respect to maintaining the security integrity of the entire installation.

b. Positive barriers exist to prevent all CTS software modifications except from specific programming and maintenance positions located within the PCZ. Maintenance diagnostics are provided from these secure positions, or from remote diagnostic support facilities in performance with the following criteria.

(1) There is no way for the RDS facility to access the CTS except through a dedicated port.

(2) The RDS port is kept disconnected from all trunks and lines leaving the PCZ when it is not in use.

(3) If ancillary equipment, such as modems or telephones, is used with the RDS procedure, it is kept disconnected from the RDS port and from the trunks and lines leaving the PCZ when the RDS is not in use.

(4) When RDS is required, it can be requested by the CTS user or by the RDS facility. In either case, the network connection between the CTS RDS port and the RDS facility must only be established by a call to the RDS facility placed through the network from a designated telephone inside the PCZ.

(5) Specifically designated personnel are responsible for ensuring the security of the RDS service. Their duties consist of performing (from within the PCZ) the following sequence each time the RDS is used.

(a) Verify that there is an immediate need for RDS.

(b) Telephone the RDS facility and verify that the support activity can begin and that the RDS facility is ready to transmit.

(c) Connect the RDS port, the ancillary equipment, and the outgoing trunks and/or lines.

(d) Dial the RDS facility to obtain the connection to the RDS port.

(e) Verify the connection with the RDS facility.

(f) If the CTS will permit, monitor in real time (with hard copy printout) all communications between the RDS facility and the CTS. Terminate the session immediately if any improper activity is observed. If the real-time monitoring and printout are not available or are not in an immediately comprehensible form, then subparagraph (h) below, must be accomplished immediately upon termination of the RDS connection. It must be recognized that subparagraph (h) may cause service interruptions in some systems and therefore, unless such interruptions are operationally and administratively acceptable (or routine RDS can be scheduled so that interruptions are acceptable), these systems cannot comply with the guidelines if they do not permit real time monitoring.

(g) At the conclusion of the session, disconnect all components specified in (3) and (4) above.

(h) If the CTS has a removable program medium (such as a magnetic tape or disk), reload the system from the safeguarded master copy. If the CTS does not have a removable program medium, perform a dump of the complete memory and compare it with the safeguarded master version.

c. Only specific designated individuals with appropriate security clearance have physical access to the programming stations and may change the system software or hardware configurations.

d. The integrity and efficacy of the protective measures are to be ensured by countermeasures inspections.

e. Frequently reload the operation program medium from the certifiable correct master to ensure that no unauthorized changes have occurred.

f. Complete copies of all systems documentation including instructions, manual, installation and service practices, system configuration records, etc., are to be kept with the CTS in the PCZ.

g. For security purposes, dial access or barrier codes are not acceptable means for denying unauthorized persons access to any CTS features or control operations.

Section III
Other Considerations

D-9. Supplementary measures

Most telephone installations of interest involve other telephone security considerations in addition to the fundamental problems of on-hook audio. Application of the supplementary measures provided in this section will enable the CTS to address those concerns; these measures are recommended whenever operationally feasible.

a. If the CTS provides any features which allow subscriber stations or attendants' consoles to monitor the audio or data at other stations (such as line or trunk verification or executive override), positive barriers are placed into the system to prevent implementing these features from outside the PCZ.

b. Central dictation features are disabled.

c. There is no CTS-accessed central loudspeaker paging system.

d. All attendants' consoles are located within the PCZ.

e. The number of central answering positions is minimized.

f. Except for attendants' consoles, all telephones are single-line 2500 type.

g. The CTS does not maintain CDR information (beyond the temporary storage that is necessary to support the communications switching functions and auxiliary features) unless positive barriers exist to preclude access to this information outside the PCZ.

h. The CTS does not maintain speed calling lists.

i. The CTS and all critical station equipment are powered from uninterruptible power supplies.

j. Service provided to facilities located outside the PCZ can be curtailed to provide priority service to internal communications

k. All switching, maintenance, or operational conditions set up from subscriber stations can be selectively cancelled by an attendant's console located within the PCZ.

Glossary

Section I
Abbreviations

AC
alternating current

ACSI
Assistant Chief of Staff for Intelligence

AMC
U.S. Army Materiel Command

APO
Army post office

ARNG
Army National Guard

ASI
additional skill identifier

AUTOSEVOCOM
automatic secure voice communications

CBX
computerized branch exchange

CCTV
closed circuit television

CDR
call detail recording

CI
counterintelligence

CKTS
computerized key telephone systems

CO
central office

COMSEC
communications security

CPBX
computerized private branch exchange

CTX
computerized telephone systems

CTSA
Certified Technical Surveillance Countermeasures special agent

DA
Department of the Army

DACOM
data communications

DC
direct current

DCI
Director, Central Intelligence

IPB
Intelligence Property Book

DCSI
Deputy Chief of Staff for Intelligence

DOD
Department of Defense

EMT
electrical metallic tubing

FCC
Federal Communications Commission

FY
fiscal year

IDS
intrusion detection system

IMA
U.S. Army Intelligence Materiel Activity

INSCOM
U.S. Army Intelligence and Security Command

IPMS
in-place monitoring system

JSIIDS
Joint Service Interior Intrusion Detection System

KSU
key service unit

KTS
key telephone service

MACOM
major army command

MOS
military occupational specialty

MTSA
Master Technical Surveillance Countermeasures special agent

OACSI
Office of the Assistant Chief of Staff for Intelligence

OADR
Originating Agency Determination Required

PABX
private automatic branch exchange

PBX
private branch exchange

PCZ
physical control zone

POM
Program Objective Memorandum

PSTN
public switched telephone network

RDS
remote diagnostic support

RF
radio frequency

RMATS
Remote Maintenance, Administration, and Traffic System

SBI
special background investigation

SCI
sensitive compartmented information

SMDR
station message detail recording

SSO
special security officer

STC
sound transmission class

TCWG
Technical Countermeasures Working Group

TDY
temporary duty

TEMPEST
compromising emanations

TSA
Technical Surveillance Countermeasures special agent

TSCM
Technical Surveillance Countermeasures

TSE
technical surveillance equipment

TSP
Telephone Security Panel

USAR
U.S. Army Reserve

USOC
universal service order code

VIP
very important person

WECO
Western Electric Company

Section II
Terms

Certified Technical Surveillance Countermeasures special agent

A TSA who has successfully completed the requirements for certification as established by Commander, INSCOM.

Master Technical Surveillance Countermeasures special agent

A CTSA who, because of exceptional standards and recognized contributions which enhance the overall TSCM program, is elevated to Master TSA.

Physical security hazard/vulnerability

A situation which, when coupled with an assessment of the sensitivity of a facility and the threat, represents a reasonable and logical opportunity or target for exploitation.

Physical/technical security weakness

A deficiency in the physical or technical security safeguards of an area that could permit access to the area by uncleared or unauthorized personnel, facilitate the installation of a technical surveillance device, or facilitate the exploitation of existing equipment characteristics to conduct a covert surveillance.

Sensitive area

An area where sensitive information (defined below) is discussed or processed on a routine basis to effectively complete the assigned mission. Usually a fixed facility which is a logical and feasible target for technical surveillance espionage.

Sensitive information

Information that requires special protection such as—

a. Sensitive compartmented information (SCI) and classified cryptographic information.

b. Other information classified at least SECRET and to which access is stringently restricted.

c. Sensitive, unclassified information which is the property of the U.S. Government or other information that can be exploited for intelligence purposes.

d. Defense information which would be of value to an enemy or potential enemy in the planning or waging of war.

Technical hazard

A condition which could permit the technical surveillance of an area because of equipment which, by reason of its normal design, installation, operation, maintenance, or damaged condition, allows or contributes to the unintentional transmission of sensitive information out of a secure area.

Technical penetration

A deliberate, unauthorized emplacement, within a target area, of a technical monitoring or intercept device or system; deliberate deviation of standard wiring or configuration; deliberate addition or removal of components to equipment; or exploitation of existing technical security hazards for the purpose of unauthorized access to sensitive information.

Technical security

Those measures taken to deny the unauthorized collection of classified or sensitive information by means of clandestine technical surveillance devices.

Technical surveillance

The employment of electronic or mechanical monitoring devices or systems against any target area of intelligence value for the purpose of gaining nonpublic information without the knowledge or consent of all parties concerned. The information gained may be classified or unclassified and may be in audio, video, or digital form.

Technical Surveillance Countermeasures special agent

A highly trained counterintelligence agent who possesses extensive knowledge in investigative, electronic, and construction skills, and has completed the U.S. Army TSCM course of instruction (formally known as Defense Against Sound Equipment—DASE) and has been awarded an additional skill identifier (ASI) of 9L for warrant officers or G9 for enlisted members.

Technical surveillance device

A mechanical or electronic device installed to monitor any nonpublic activities within a target area, most often to seek sensitive information. Normally such installations are made at the direction of a hostile foreign intelligence service.

TSCM certification program

A program designed to establish minimum qualification standards for personnel who conduct TSCM investigations.

TSCM equipment

A limited group of special items of electronic equipment or other materiel specifically designed or modified for use in TSCM investigations for the detection or neutralization of audio, visual, or other technical means to obtain sensitive information. Excluded from this category are technical items not specifically designed or modified for TSCM, but which are used to augment or supplement TSCM equipment.

TSCM inspection

A follow-up to a TSCM survey but may be limited in scope. The service is directed more at direct threat posed to the sensitive area or modifications that have been made to an area after the conduct of a TSCM survey; or when time or local conditions preclude conduct of a comprehensive survey.

Penetration/hazard investigation

A CI investigation of an actual or suspected technical penetration or hazard conducted by TSCM personnel.

Preconstruction technical advice and assistance

A service conducted prior to or during construction or renovation of an existing sensitive area to ensure that appropriate physical and technical security safeguards are included in planning.

TSCM survey

A thorough physical, electronic, and visual examination by TSCM personnel in and about an area to detect technical surveillance devices, technical surveillance hazards, and physical and technical security deficiencies which would facilitate the placement of technical surveillance devices or systems.