

30 April 2004

Security

Technical Counterintelligence Services

*This regulation supersedes USAREUR Regulation 380-85, 3 May 1994.

For the CG, USAREUR/7A:

E. PEARSON
Colonel, GS
Deputy Chief of Staff

Official:



GARY C. MILLER
Regional Chief Information
Officer - Europe

Summary. This regulation establishes policy and prescribes procedures for requesting counterintelligence services.

Applicability. This regulation applies to—

- USAREUR organizations and activities.
- Organizations supported by USAREUR.

Supplementation. Organizations will not supplement this regulation without USAREUR G2 (AEAGB-SAD-S) approval.

Forms. This regulation prescribes AE Form 380-85A and AE Form 380-85B. AE and higher-level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System Web site at <https://www.arims.army.mil>.

Suggested Improvements. The proponent of this regulation is the USAREUR G2 (AEAGB-SAD-S, DSN 370-6564/8179). Users may send suggestions to improve this regulation on DA Form 2028 to the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351.

Distribution. B (AEPUBS).

CONTENTS

1. Purpose
2. References
3. Explanation of Abbreviations and Terms
4. Responsibilities
5. Policy
6. Request for TCI Services
7. Coordination
8. Security Violations and Deficiencies
9. Reports
10. TCI Schedules for Inspection
11. Corrective Actions
12. Counter-Signals Intelligence Services
13. TEMPEST Services

Appendixes

- A. References
- B. Technical Surveillance Countermeasures Investigations
- C. Counterintelligence Offices
- D. Security Procedures for Classified Meetings and Conferences
- E. Sample Request for a TCR

Glossary

1. PURPOSE

This regulation—

- a. Describes technical counterintelligence (TCI) services.
- b. Prescribes policy and procedures for requesting TCI services.
- c. Does not apply to providing physical-security services except in areas used for classified discussions or classified workareas.
- d. Prescribes policy and procedures to protect classified information from being compromised.
- e. Prescribes policy and procedures to protect what information from technical surveillance, technical hazards, or both.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary explains abbreviations and terms.

4. RESPONSIBILITIES

- a. The USAREUR G2 (AEAGB-SAD-S) will—
 - (1) Establish—
 - (a) A TCI services program in USAREUR.
 - (b) Policy for TCI services.
 - (2) Coordinate requests for TCI services from HQ USAREUR/7A staff offices, USAREUR major subordinate and tenant commands (AE Reg 10-5), and attached and supported units.

(3) Coordinate TCI support from other armed services in regions where the Army does not have primary TCI responsibility.

(4) Consider requests for TCI services not described in this regulation.

(5) Direct requests for TCI services to the appropriate activity or office (for example, 66th Military Intelligence Group (66th MI Gp), USAREUR G3 Information Operations Office).

(6) Distribute information about deficiencies noted while conducting TCI services.

b. The 66th MI Gp provides TCI service support to HQ USAREUR/7A staff offices, USAREUR major subordinate and tenant commands, attached and supported units, area support groups, and base support battalions.

c. V Corps will provide counterintelligence (CI) services to V Corps and V Corps-supported units using assigned CI assets.

(1) V Corps CI services do not include technical surveillance countermeasures (TSCM) (AR 381-14), TEMPEST, or counter-signals intelligence (C-SIGINT) support.

(2) When the requirements for CI services to V Corps units exceed the capability of assigned CI assets, V Corps may request additional support from the USAREUR G2 (AEAGB-SAD-S), Unit 29351, APO AE 09014-9351. An information copy of the request must be sent to the 66th MI Gp (IAPG-OP), Unit 29500, APO AE 09175-9500.

5. POLICY

a. The USAREUR G2 is the proponent for TCI services in USAREUR areas of responsibility (AORs). Security managers will identify the need for TCI services and send requests to appropriate commanders. Commanders of supported units will—

(1) Consolidate TCI needs.

(2) List TCI services requested for the upcoming fiscal year. The list—

(a) Should be in order of priority.

(b) Is due 1 February each year to the USAREUR G2 with an information copy sent to the 66th MI Gp (para 4c(2) provides addresses).

b. TCI advice and assistance may be informal when responding to the needs of requesting units. Units may request advice from the supporting TCI element by telephone or in writing. Security managers will not include requests for advice and assistance in the consolidated annual list (a above).

c. Security managers will establish procedures to conduct announced, unannounced, and after-duty-hour inspections. The serviced unit will keep results of inspections for use during future TCI services. After-duty-hour inspections should be incorporated into the unit's security manager inspection program.

d. Appendix B provides TSCM policy.

6. REQUESTS FOR TCI SERVICES

a. Requests for TCI services must be in writing and sent through command channels to the USAREUR G2 with a copy of requests sent to the 66th MI Gp (para 4c(2) provides addresses). Requirements for access to special-category material must be specified in the request. Security managers and information assurance managers at each level will review requests and do one of the following:

(1) Recommend approval and forward the request to the next level in the chain of command.

(2) Disapprove the request and return it to the originator.

b. Security managers and information assurance managers will send time-sensitive, emergency requests for 66th MI Gp CI services by message to—

(1) CDRUSAREUR DCSINT HEIDELBERG GE and CDRUSAREUR HEIDELBERG GE//AEAGB-SAD-S// and CDR66THMIGP DARMSTADT GE//IAPG-OP//.

(2) If using Defense Messaging System (DMS): ou=USAREUR G2(uc), ou=USAREUR 7A, l=EUROPE, ou=Organizations, ou=Army, ou=DOD, o=U.S. Government, c=US and ou=CDR66MIGP(uc), ou=66THMIGP, ou=USAINSCOM, l=EUROPE, ou=Organizations, ou=Army, ou=DOD, o=U.S. Government, c=US.

(3) Intermediate commands (as information addressees).

c. The procedure in subparagraph b above will not be used to avoid normal requesting procedures. The requesting activity should be prepared to fund unscheduled and unprogrammed requests for any TCI service.

d. Emergency requests must explain when the service is needed, include a justification, explain the urgency, and be signed by the first colonel (O6) in the requester's chain of command.

e. The USAREUR G2, in coordination with the 66th MI Gp, has final approval authority on requests for TCI service.

f. Appendix B explains procedures for requesting TSCM services.

g. AR 381-14 provides TEMPEST policy, responsibilities, and assessment requirements to control compromising emanations. Paragraph 13 (this reg) explains TEMPEST services. Appendix E (this reg) shows documents required for a request for a TEMPEST countermeasures review (TCR).

h. Field Manual 34-60 describes C-SIGINT. Paragraph 12 (this reg) and AE Regulation 380-53 explain C-SIGINT services.

i. Appendix C lists locations and telephone numbers of 66th MI Gp CI offices. Units may contact these offices for information on available TCI support.

j. Requests for services covered by this regulation will be classified according to—

(1) This regulation, appendix B.

(2) Director of Central Intelligence Directive 6/9.

(3) ARs 25-2, 380-5, 380-53, 381-14, and 381-20.

(4) Other derivative authority (for example, AR 380-5).

(5) The sensitivity of the information in the request.

7. COORDINATION

a. TCI service requests sent to the USAREUR G2 must include the name, grade, location, and telephone number of the unit POC. After the request has been validated by the USAREUR G2 (AEAGB-SAD-S), the 66th MI Gp supporting element will—

(1) Coordinate with the POC.

(2) Determine what services will be provided and ensure resources are available.

(3) Develop an operational concept or operation plan, as required.

(4) Determine other requirements to complete the mission (for example, security clearances, directives, governing documents unique to the unit and the service requested).

b. After personnel performing authorized or requested TCI services present their credentials, the requesting unit will ensure the personnel are not—

(1) Unduly delayed.

(2) Refused or restricted in access to material or entry to areas requiring TCI services.

8. SECURITY VIOLATIONS AND DEFICIENCIES

Persons conducting TCI services will report possible losses or compromises of classified material according to AR 380-5. The TCI service report will include the possible loss or compromise as a finding and indicate an appropriate recommendation.

9. REPORTS

a. The supporting CI element will send reports of the TCI services provided under paragraph 4c to the USAREUR G2 (para 4c(2) provides the address).

b. When services are completed, the supporting CI element will brief the unit commander or designated representative.

c. Classified inspection and investigation reports will be marked according to AR 380-5, USAREUR Supplement 1 to AR 380-5, and other governing regulations.

10. TCI SCHEDULES FOR INSPECTION

After an initial investigation, TSCM investigation, C-SIGINT and TEMPEST services will be scheduled as required, based on requests and priorities. Facilities will not be scheduled for automatic annual or periodic reinvestigations.

11. CORRECTIVE ACTIONS

a. V Corps will send reports of corrective action taken on TCI services conducted under paragraph 4c within 90 days to the USAREUR G2 (para 4c(2) provides the address).

b. Reports requiring corrective actions resulting from TEMPEST inspections, TSCM investigations, and TCI inspections will be sent through command channels to the USAREUR G2 with an information copy sent to the 66th MI Gp (para 4c(2) provides addresses). The report of corrective action must be sent to arrive within 60 days after the date of the CI service report. Commanders of supported units will ensure inspection reports are signed by the responsible commander or are accompanied by a statement that the commander has reviewed and concurs with the corrective actions taken.

c. HQ USAREUR/7A staff offices will send reports of corrective actions on an informal memorandum to the USAREUR G2 (AEAGB-SAD-S) within 60 days after the report date.

d. If the initial report of a TCI service shows a possible compromise or loss of classified material, the report of corrective action will refer to the initial report (b or c above) or include a summary of the action taken and the results.

12. COUNTER-SIGNALS INTELLIGENCE SERVICES

a. C-SIGINT distinguishes between signals security (SIGSEC) and CI activities that support SIGSEC. C-SIGINT is intelligence support for a command's SIGSEC and operations security (OPSEC) programs. C-SIGINT has the following support functions:

(1) Countermeasures evaluation.

(2) Countermeasures recommendations.

(3) Threat assessment.

(4) Vulnerability and risk assessment.

b. Information systems security monitoring may be included in the C-SIGINT process during the evaluation phase (AE Reg 380-53).

c. AE Regulation 380-53 provides procedures for requesting C-SIGINT services.

13. TEMPEST SERVICES

a. Support-Level Determination. Use the decision flowchart in AR 381-14, figure 4-2, to determine the appropriate level of TEMPEST support required.

b. TEMPEST Inspection.

(1) A TEMPEST inspection will be conducted at facilities that electronically process classified information. The inspection is a desktop review of the facility technical threat assessment (FTTA).

(2) The FTTA will be completed according to AR 381-14, paragraphs 2-2 and C-3. Preparation of the FTTA is required for commanders who establish or plan to alter, expand, or relocate facilities or systems to process classified information electronically.

(3) Unit certification agents or information assurance managers will submit the completed FTTA to the USAREUR G2 (AEAGB-SAD-S) at g2tso@dcsint.hqsareur.army.smil.mil (or secure fax at DSN 370-8455) and the 66th MI Gp (IAPG-DI-T) at 66MIGPTSCM@exchange.66mi.army.smil.mil in support of a commander's certification and accreditation of classified systems.

(4) Based on a review of the FTTA, the Chief, TCI Branch, 66th MI Gp, will provide a memorandum of concurrence or nonconcurrence and recommend countermeasures when appropriate. Recommended countermeasures must be implemented and certified by the unit or activity security manager or information assurance manager. Failure to implement the recommended countermeasures is a reportable security incident under this regulation. The FTTA and TCR will be a subject of interest during inspections and staff assistance visits. Additional TEMPEST support, if required (for example, on-site inspection, verification, or TEMPEST-instrumented test), that cannot be provided by an Army in Europe certified TEMPEST technical authority (CTTA) will be scheduled by the United States Army Intelligence and Security Command (INSCOM) support element at Fort Meade, Maryland, in coordination with the supported command.

(5) Activities may request telephonic advice for completing the FTTA from the 66th MI Gp at DSN 348-7773/6735.

c. TEMPEST Test. A TEMPEST test is conducted at operational facilities using test instruments. A TEMPEST test will be conducted only when warranted. The commander of the INSCOM support element will determine the need for a TEMPEST test based on the—

- (1) TEMPEST inspection.
- (2) Recommendation of the USAREUR CTTA (66th MI Gp).
- (3) Review of the FTTA.
- (4) Facility or system vulnerability and sensitivity.

d. Unscheduled TEMPEST Support.

(1) Units with a compelling need and strong justification may request unscheduled TEMPEST support for review and validation. Requests will be sent to the USAREUR G2 (AEAGB-SAD-S/Technical Security Officer), Unit 29351, APO AE 09014-9351. Information copies will be sent to the following:

- (a) 66th MI Gp (IAPG-OP), Unit 29500, APO AE 09175-9500.
- (b) 66th MI Gp (IAPG-DI-T), Unit 29500, APO AE 09175-9500.
- (c) Other appropriate persons in the chain of command.

(2) The requesting unit must be prepared to fund unprogrammed TEMPEST support. Requests for such support should include a fund citation to defray temporary duty expenses.

(3) Requests for unscheduled TEMPEST support will include at least the following:

(a) Dates and results of previous services.

(b) The name of the facility or system to be inspected.

(c) When the service is requested.

(d) A justification.

(e) Explanation of the urgency.

(f) Signature the first colonel (O6) in the requestor's chain of command.

(g) POC information (local TEMPEST coordination officer, information systems security officer, information systems security manager, security manager, or information assurance manager).

(h) Description of service needed.

(4) Once validated by the USAREUR G2 (AEAGB-SAD-S), requests for unprogrammed TEMPEST support will be arranged by priority based on the requesting activity's need and available resources.

APPENDIX A REFERENCES

SECTION I PUBLICATIONS

Committee on National Security Systems Policy No. 300, National Policy on Control of Compromising Emanations

National Security Telecommunications Information Systems Instruction 7000, TEMPEST Countermeasures for Facilities

National Security Telecommunications Information Systems Security Advisory Memorandum TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements, Electromagnetics

National Security Telecommunications Information Systems Security Advisory Memorandum TEMPEST/1-93, Compromising Emanations Field Test Requirements, Electromagnetics

National Security Telecommunications Information Systems Security Advisory Memorandum TEMPEST/2-95, Guidelines for Facility Design and RED/BLACK Installation

NOTE: On 16 October 2001, the National Security Telecommunication Information Systems Security Committee was redesignated as the Committee on National Security Systems. See <http://www.nstissc.gov> for more information.

Director of Central Intelligence Directive 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities

DOD Directive 8100.2, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

DOD Instruction 5240.5, DOD Technical Surveillance Countermeasures (TSCM) Survey Program

AR 25-2, Information Assurance

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 380-5 and USAREUR Supplement 1, Department of the Army Information Security Program

AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 381-14, Technical Counterintelligence (TCI)

AR 381-20, The Army Counterintelligence Program

AR 380-53, Information Systems Security Monitoring

Field Manual 34-60, Counterintelligence

AE Regulation 10-5, HQ USAREUR/7A Organization and Responsibilities

AE Regulation 190-13, Army in Europe Physical Security Program

AE Regulation 380-40, Safeguarding and Controlling Communications Security Material

AE Regulation 380-53, Information Systems Security Monitoring

SECTION II FORMS

DA Form 2028, Recommended Changes to Publications and Blank Forms

DA Form 7453, Facility Technical Threat Assessment (FTTA) Worksheet

AE Form 385-85A, Request for TSCM Support

AE Form 385-85B, Army Facility/System TEMPEST Questionnaire

APPENDIX B

TECHNICAL SURVEILLANCE COUNTERMEASURES INVESTIGATIONS

B-1. PURPOSE

This appendix prescribes policy and procedures for requesting, classifying, and reporting technical surveillance countermeasures (TSCM) investigations in the Army in Europe.

B-2. POLICY

The Army in Europe TSCM Program includes measures taken to reduce vulnerability to technical surveillance threats.

a. A secure facility is an area that—

- (1) Complies with AR 381-14 and Director of Central Intelligence Directive 6/9 security standards.
- (2) Corrected previously identified deficiencies.

b. Plans for constructing or modifying sensitive areas will incorporate physical and technical security standards established in AR 381-14 and Director of Central Intelligence Directive 6/9. The organization constructing or modifying a sensitive area should arrange TSCM advice and assistance support early in the planning cycle.

c. To protect the validity of TSCM investigations in the serviced areas, references to requesting, planning, and conducting TSCM investigations will be in writing and classified Secret in accordance with AR 381-14. The compromise of a TSCM investigation is a serious security violation. These investigations will not be discussed until they are completed. All personnel who are involved in the process of providing or receiving TSCM services are required to exercise appropriate operational security measures to ensure the success and effectiveness of the countermeasures effort. If discussions about the pending support take place in the sensitive area to be investigated, any clandestine surveillance device would most likely be deactivated or removed before the investigation and later reactivated or reinstalled. For this reason, no discussion or verbal comments about pending support or travel destinations of TSCM agents should be permitted in the areas to be serviced.

B-3. PROCEDURES

a. A TSCM investigation is—

(1) Conducted to detect and neutralize technical surveillance devices targeted against USAREUR sensitive and secure areas, distinguished visitor travels and offices, vehicles (to include aircraft), and conferences.

(2) Preventive, because it will identify and correct technical and physical security vulnerabilities and provide commanders with a comprehensive vulnerability assessment of a facility's technical and physical security posture. Compliance with the investigation will make it more difficult to install covert devices.

(3) Helpful, because electronic equipment used in everyday work has inherent security weaknesses. These hazards may be easily exploited for the purpose of collecting the sensitive or classified information being processed. These weaknesses can occur through normal design characteristics of the equipment, damage to the equipment, normal wear and aging of the equipment, or the equipment can be deliberately modified to produce a vulnerability while continuing to operate normally. A TSCM investigation can identify these hazards and make the facility a more secure working facility.

(4) Time-consuming, because TSCM investigations involve a physical search and use of technical equipment. TSCM investigations also impose some minor requirements on the requester. (For example, the requester must ensure the serviced area remains protected from unauthorized visitors, and a large desk for working space and a storage area for TSCM equipment must be provided.)

(5) Not intrusive, because the office should be working as normal. Changing, stopping, or severely curtailing normal business could reveal that a TSCM investigation is in progress or is about to begin. That, in turn, could result in the surveillance device being turned off or removed from the facility, making its discovery more difficult.

b. Before requesting a TSCM investigation, the commander should consider the following:

(1) The passage of time is not justification for repeating a TSCM investigation. The limited technical service assets in the Army in Europe require that TSCM investigations be—

(a) Conducted selectively.

(b) Based on a valid need for the investigation according to the facility technical threat assessment (FTTA) (see AR 381-14, paras 2-2 and 3-4).

(2) Throughout the TSCM investigation, the facility commander or responsible security official must be prepared to—

(a) Maintain positive access control and exclude unauthorized or uncleared persons from entry unless personnel familiar with the security requirements of the area continuously escort them.

(b) Maintain continuous and effective surveillance and control of the area.

(c) Have repairs or alterations to the area supervised and closely monitored. Personnel should be briefed to watch for attempts at installation of devices or the presence of unusual or unexplained equipment.

(d) Have new furnishings or equipment thoroughly inspected by qualified security or appropriately cleared maintenance personnel.

c. A limited TSCM investigation may be conducted on a one-time basis if classified material will be discussed in a nonsecure facility. This type of in-conference investigation will be conducted only at the discretion and with the approval of the USAREUR G2 (AEAGB-SAD-S). Normally, the investigation will be done the day of the classified discussion. The security precautions in appendix D will apply. The service will become invalid immediately after the facility is used.

d. Requests for TSCM investigations will—

(1) Be classified at least Secret (AR 381-14).

(2) Submitted on AE Form 380-85A. An electronic copy of this form is available from at <https://aepubs.army.mil> or at <http://www.66mi.army.smil.mil/di/tscm.html>.

(3) Be signed or endorsed by the first colonel (O6) in the requestor's chain of command.

(4) Include DA Form 7453. AR 381-14 provides detailed instructions for completing DA Form 7453.

(5) Be sent to the USAREUR G2 (AEAGB-SAD-S) at g2tso@dcsint.hqusareur.army.mil (or secure fax at DSN 370-8455). Check the 66th Military Intelligence Group (66th MI Gp) TSCM Web page (<http://www.66mi.army.smil.mil/di/tscm.html>) for the latest requesting procedures.

e. Each person in the chain of command will review requests for technical services to ensure the requests comply with this appendix. Commanders at intervening command levels will disapprove requests if no valid basis for the request exists or if the requester failed to comply with requirements. If disapproved, the request will be returned to the originator.

f. Once the request for a TSCM investigation has reached HQ USAREUR/7A and been validated by the USAREUR G2 (AEAGB-SAD-S), it will be added to the calendar. A tentative timetable for the investigation may be discussed with the Chief, Technical Counterintelligence (TCI) Branch, 66th MI Gp, at DSN 348-7773.

g. No facility will qualify automatically for recurrent TSCM investigations. Recurrent investigations in a facility will be conducted only if the TCI Chief, based on a documented threat and vulnerabilities assessment of the facility, considers such investigations appropriate. This determination will be based on the threat level, sensitivity of information, and the susceptibility of the facility to technical penetration. AR 381-14 provides the following guidelines:

(1) Priority 1. TCI investigation of suspected or confirmed technical penetrations and technical security hazards, including hardware modifications or anomalies found in computer systems and networks.

(2) Priority 2.

(a) TCI investigation of facilities or activities for which technical collection and nontraditional adversarial threats are assessed as high.

(b) Travel support. Residences, hotels, and vehicles of distinguished visitors (DVs) or senior officers, when operational requirements dictate that classified information must be discussed or processed in high- or medium-threat environments.

(c) In-conference monitoring. Real-time support of events held in a location for which the technical collection threat is assessed as high. This term applies to support given to conferences, negotiations, exercises, seminars, training courses, or other events of specified time, location, and duration.

(d) Preconstruction technical advice and assistance.

(e) In a tactical environment where U.S. Forces occupy spaces recently used by opposing forces or former belligerents.

(3) Priority 3.

(a) TSCM investigation of offices, secure conference areas, and other sensitive areas for which the technical threat is assessed as medium or low.

(b) In-conference monitoring in medium- or low-threat environments.

(c) Travel support. Residences, hotels, and vehicles of DVs or senior officers, when operational requirements dictate that classified information must be discussed or processed in low-threat environments.

(4) Priority 4.

(a) All other missions based on the level of threat, degree of sensitivity, and vulnerability of the facility.

(b) Technical evaluations and equipment inspections.

(5) Priority 5.

(a) TSCM cross-service support. TSCM support will be provided by the Army to the facilities or activities of other military departments on a nonreimbursable basis, in accordance with cross-servicing agreements approved by the DA G2.

(b) Direct special support. Activities of certain high-level DOD and DA authorities or organizations are considered to have a sensitivity that warrants special TSCM support. These requirements will be identified by the DA G2 and validated by the United States Army Intelligence and Security Command Technical Surveillance Program Director.

(c) Non-DOD Government. Requests from non-DOD Government departments will be referred to the DA G2 for consideration.

h. Requesting units must be prepared to fund unprogrammed TSCM support. Requests for such support must include a fund citation to defray temporary duty expenses.

(1) These requests must state when the service is needed, include a justification, explain the urgency, and be signed by the first colonel (O6) in the requester's chain of command.

(2) Once validated by the USAREUR G2 (AEAGB-SAD-S), requests for unprogrammed TSCM support will be arranged by priority based on the requesting activity's need and available resources.

B-4. ACTION ON DISCOVERY OF A SUSPECT DEVICE

a. The discovery of an actual or suspected technical surveillance device must be reported immediately using secure means to the TSCM Section, 66th MI Gp. All information about the discovery will be handled as Secret. Installation or unit security managers will request an immediate investigation by supporting TSCM special agents.

b. The discovery of possible technical surveillance devices demands immediate action. The following procedures apply:

(1) Stop all classified activity immediately.

(2) Immediately report the discovery using secure means in accordance with AR 381-12 to the local supporting counterintelligence office or S2.

(3) Do not report it from within the facility or on facility telecommunications systems.

c. Detailed reporting and investigating procedures are governed by the USAREUR Standard Operating Procedures for Counterintelligence Investigations and Related Matters (available from the USAREUR G2 (AEAGB-SAD-S)), AR 381-14, and National Security Presidential directives.

B-5. CLASSIFICATION

a. Information pertaining to the TSCM Program must be given appropriate protection to preserve the integrity of the information and the program. As a minimum, TSCM information must be classified as follows:

(1) Correspondence or documentation that indicates the date and specific location of pending TSCM activity will be classified at least Secret/NOFORN but may be downgraded to Confidential after the TSCM activity.

(2) Technical reports and correspondence pertaining to major security vulnerabilities will be classified Secret/NOFORN. Minor security vulnerabilities normally will be classified Confidential.

(3) Information that refers to the discovery or alleged discovery of a clandestine technical penetration will be classified at least Secret/NOFORN.

(4) The classification authority will be cited as follows:

DERIVED FROM: DOD INSTRUCTION 5240.5
DECLASSIFY ON: X1.
DATE OF SOURCE: 23 MAY 1984

b. Written requests for TSCM services must be handled at the Secret/NOFORN level or above. TSCM personnel will disregard requests received through nonsecure means. Secure telephone requests for TSCM investigations from within the affected facility compromise the TSCM support.

c. Security managers and information assurance managers of facilities must be reminded of the following:

(1) The fact that the facility has been scheduled for a TSCM investigation is classified at least Secret/NOFORN.

(2) Pending TSCM investigations will not be discussed within the facility or on facility telecommunications systems. The use of a secure telephone unit, third generation (STU III), or secure telephone equipment (STE) does not negate this requirement. A listening device installed in the vicinity of a STU III or STE will still pick up and transmit the conversation.

(3) Only personnel with a need-to-know may be informed of TSCM team visits. Personnel who have a need to know must be made aware of the seriousness of compromising information about these visits and warned not to talk about them and not to try talking around the specifics of the visit.

d. If a TSCM investigation is compromised, the special agents will terminate the investigation at once. The circumstances surrounding the compromise of the investigation will be reported to the commander of the supported facility. The TSCM investigation will not be rescheduled until the cause and effect of the compromise has been evaluated.

B-6. REPORTS

The investigating team will provide a copy of the report to the serviced unit and the Army in Europe Technical Security Officer, Office of the USAREUR G2 (AEAGB-SAD-S). Copies of inspection reports must be kept in local records in accordance with AR 25-400-2, and distributed according to AR 381-14.

**APPENDIX C
COUNTERINTELLIGENCE OFFICES**

66th Military Intelligence Group Detachments and Offices	DSN Number	Civilian Number
Spy Hot Line	347-3479	06155-60-3479
Bad Aibling	441-3700	08061-80-3700
	After duty hours	0170-4514190
Belgium	361-5539/5408	0032-6827-5408
	After duty hours	0032-47657-5733
Benelux	364-6150	0031-45-563-6150
	After duty hours	0031-65-152-9985
Darmstadt	348-6933/6935	06151-696933
	After duty hours	0170-9271154
Grafenwöhr	475-7765/6	09641-83-8420
	After duty hours	0171-5522795
Hanau	322-9187/8697/8816	06181-888697
	After duty hours	0171-2232731
Heidelberg	370-6781-8252	06221-57-6781
	After duty hours	0171-3001494
Hohenfels	466-4682	0947-283-4682
	After duty hours	0175-2638060
Kaiserslautern	489-7080/7325	0631-536-7080
	After duty hours	0171-5522793
Livorno	633-7777	050-547777
	After duty hours	0335-7125264
Mannheim	381-8276/8663	0621-730-8276
	After duty hours	0171-3001494
Schweinfurt	354-6876	
	After duty hours	0171-3001492
Stuttgart	421-2206/2207	0711-729-2206
	After duty hours	0171-2258251
Vicenza	634-8030/7687/7660	0444-517660
	After duty hours	0335-7124263
Wiesbaden	337-5384	0611-7055384
	After duty hours	0171-2232731
Würzburg	351-4317/4217	0931-296-4317
	After duty hours	0171-3001492

NOTE: Telephone numbers are subject to change. Check <http://www.66mi.army.smil.mil/di/oceci/> for up-to-date information.

APPENDIX D

SECURITY PROCEDURES FOR CLASSIFIED MEETINGS AND CONFERENCES

D-1. SITE PREPARATION

Classified briefings or discussions often have to be conducted at a location that has not had a TSCM investigation (for example, the audience is too large for a secure facility or a secure area is not available because of scheduling conflicts). In these cases, classified discussions may take place in nonsecure facilities, excluding facilities identified in AR 380-5. When using nonsecure facilities, commanders will—

a. Select a U.S. facility that has had the most protection in the past (for example, a conference facility located on a guarded installation where access is controlled during the day and the building is locked at night). Theaters, officer and enlisted soldier clubs, and facilities generally open to the public must be avoided.

b. Control access to the entire physical perimeter of the facility, including ceilings, floors, and walls. Guards will—

(1) Be present during classified discussions.

(2) Be positioned to observe all sides of the facility and prevent unauthorized persons from approaching within eavesdropping range.

(3) Have security clearances. If the guards do not have appropriate clearances, they must be stationed so they cannot overhear classified discussions.

c. Check surrounding rooms to ensure natural and amplified voices cannot be heard in them. If this problem cannot be corrected, cleared guards should be stationed in the surrounding rooms to prevent the rooms from being used during classified discussions.

d. Control access to classified discussions to ensure participants have the required security clearance and a valid need to participate.

e. Not announce the times and places of classified discussions in unclassified media or over nonsecure telephones.

f. Ensure no wireless microphones or communication devices are used during the classified portions of the briefing or conference.

D-2. RADIO FREQUENCY DEVICES

Radio frequency (RF) devices are prohibited from all classified processing areas unless a verified operational need exists and use of the RF devices was approved by a certified TEMPEST technical authority (CTTA). RF devices include cell phones, some personal data assistants, radio transmitters (ultra high frequency (UHF), very high frequency (VHF), low-to-medium range (LMR), high frequency (HF), citizens band (CB), and RF peripherals, such as wireless keyboards, mice, and microphones regardless of whether they are used on RED or BLACK equipment). If an operational need exists, follow the guidance in National Security Telecommunications Information System Security Advisory Memorandum TEMPEST/2-95A, section 3.

APPENDIX E
SAMPLE REQUEST FOR A TCR

This appendix is a sample of a request packet for TEMPEST countermeasures review (TCR). The samples in this appendix are all unclassified. Classification markings are for demonstration purposes only.

DA Form 7453 is classified Secret only when completed for TSCM. When using the form as part of the TEMPEST TCR packet, only the protective marking FOR OFFICIAL USE ONLY is used. The information shown in samples in this appendix is Unclassified and provided for demonstration purposes only.

CLASSIFIED WHEN FILLED-IN					
FACILITY TECHNICAL THREAT ASSESSMENT (FTTA) WORKSHEET					
For use of this form, see AR 381-14; the proponent agency is ODCS, G-2. (Instructions for completing this form are on the back).					
1. FULL MILITARY/OFFICIAL MAILING ADDRESS 50th Transportation Battalion (AEAGT-S-IM) Unit 09111 APO AE 09000-9111			2. PHYSICAL LOCATION OF FACILITY Building 2000 Camp Dogwood Wiesbaden, GE		
3. FACILITY IDENTIFICATION NUMBERS/SCIF ID NA		4. PRIMARY USE OF FACILITY, EQUIPMENT OR SYSTEM Office		5. SIZE OF FACILITY 275 Sq. Ft.	
6. VOLUME AND SENSITIVITY OF INFORMATION					
% OF TOTAL	LEVEL OF DISCUSSION OR PROCESSING	% LONG TERM	% SHORT TERM	HOURS/MONTH	
100	Secret Collateral	20	80	40	
7. EQUIPMENT CONFIGURATION <i>(additional items can be listed on the back)</i>					
a. List of Equipment Used	b. Within 30 Meters (if yes, complete block 7)		Name of Manufacturer for the Transmitter and the Antenna	Model Number for the Transmitter and the Antenna	Power Output of the Transmitter
	Yes	No			
Systemax Venture Desktop Computer					
DeskJet 320					
c. For TSCM Only (List the manufacturer and model, of telephone switching equipment inside the facility)					
Manufacturer			Model	Number of Telephones	
8a. NAME OF POINT OF CONTACT ILT Jonathan Morales			b. TITLE OF POINT OF CONTACT Information Management Officer		
c. MAILING ADDRESS OF POINT OF CONTACT AEAGT-S-IM Unit 09111, APO AE 09000-9111			d. E-MAIL ADDRESS moralesj@hq.hqusaureur.army.mil		
9. SIGNATURE OF POINT OF CONTACT (Should be signed by the same person as the cover memorandum)				DATE (YYYYMMDD)	

DA FORM 7453, SEP 2002

CLASSIFIED WHEN FILLED-IN

USAPA V1.00ES

CLASSIFIED WHEN FILLED-IN

ADDITIONAL SPACE IF NEEDED

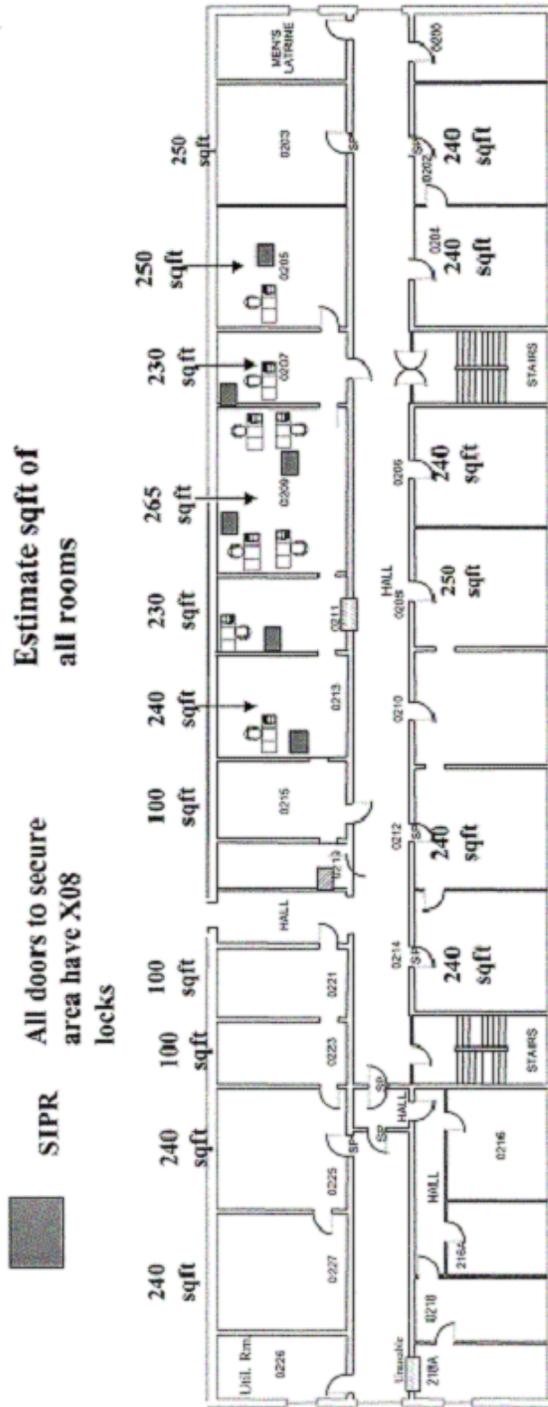
INSTRUCTIONS FOR COMPLETION OF DA FORM 7453

1. Item 1. Full Military Official Mailing Address.
2. Item 2. Physical Location of Facility. Exact physical location of the activity, facility, building, equipment, or system for which support is requested. Include building and room numbers, and street names. Indicate if the facility is on a US military base, or US government-owned or leased facility that is occupied totally by US Government personnel. Attach a sketch of the facility's location and immediate environment, denoting its IS.
3. Item 3. Facility Identification Numbers. Provide the Facility Identification Number (FIN), if one has been assigned. If the activity is a Sensitive Compartmented Information Facility (SCIF), provide the SCIF number.
4. Item 4. Primary Use of the Facility Equipment, system, or area to be examined (i.e., office, conference room, and telecommunications center).
5. Item 5. Size of Facility. Size of facility in square feet of floor space within the targeted facility perimeter.
6. Item 6. Volume and Sensitivity of Information. Provide the information about the volume and sensitivity of the information processed. Figures should be the monthly average. The percentages for long-term and short item at a given sensitivity level should add up to 100%
7. Item 7. Equipment Configuration.
 - a. Submit a list of all equipment used to process classified information by manufacturer and model number. Describe any networks that exit the facility, whether processing classified or unclassified information.
 - b. If there is a transmitter or transmitting antenna of any type located within 30 meters of the equipment, system, or facility, provide the name of the manufacturer and model number for the transmitter and the antenna, and the power output of the transmitter.
 - c. (For TSCM Only) Provide the manufacturer and model of telephone switching equipment inside the facility. List the number of telephones, by model, located inside the facility.
8. Item 8. Name of Point of Contact. Point of contact for the request. Name, position title, mailing address, telephone number and if available, a secure email address, of individual who has security responsibility for the area and who will act as the point of contact.
9. Item 9 Signature. Should be signed by the same person as the cover memorandum. The position title in the signature block should clearly indicate that the signatory has authority to request TSCM (Commander, Security Officer, MACOM TSO, etc.)

BACK, DA FORM 7453, SEP 2002

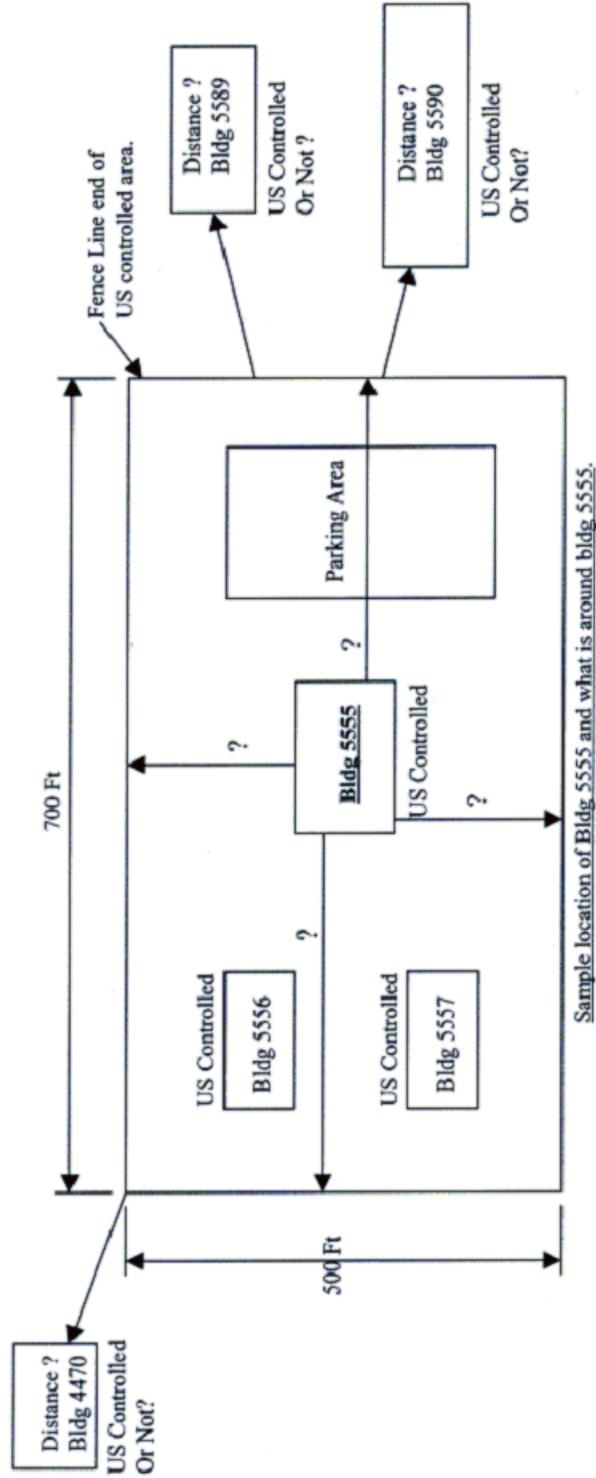
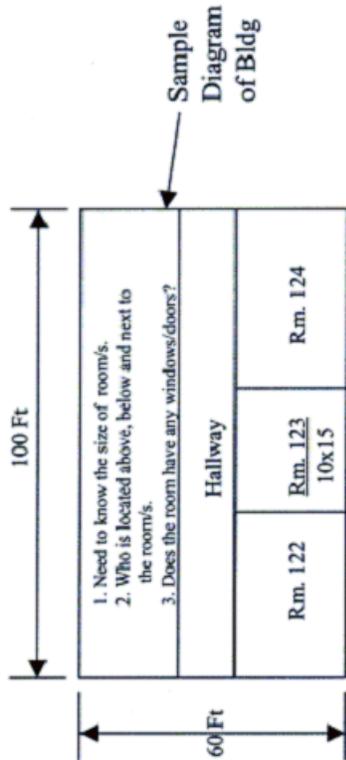
USAPA V1.00ES

CLASSIFIED WHEN FILLED-IN

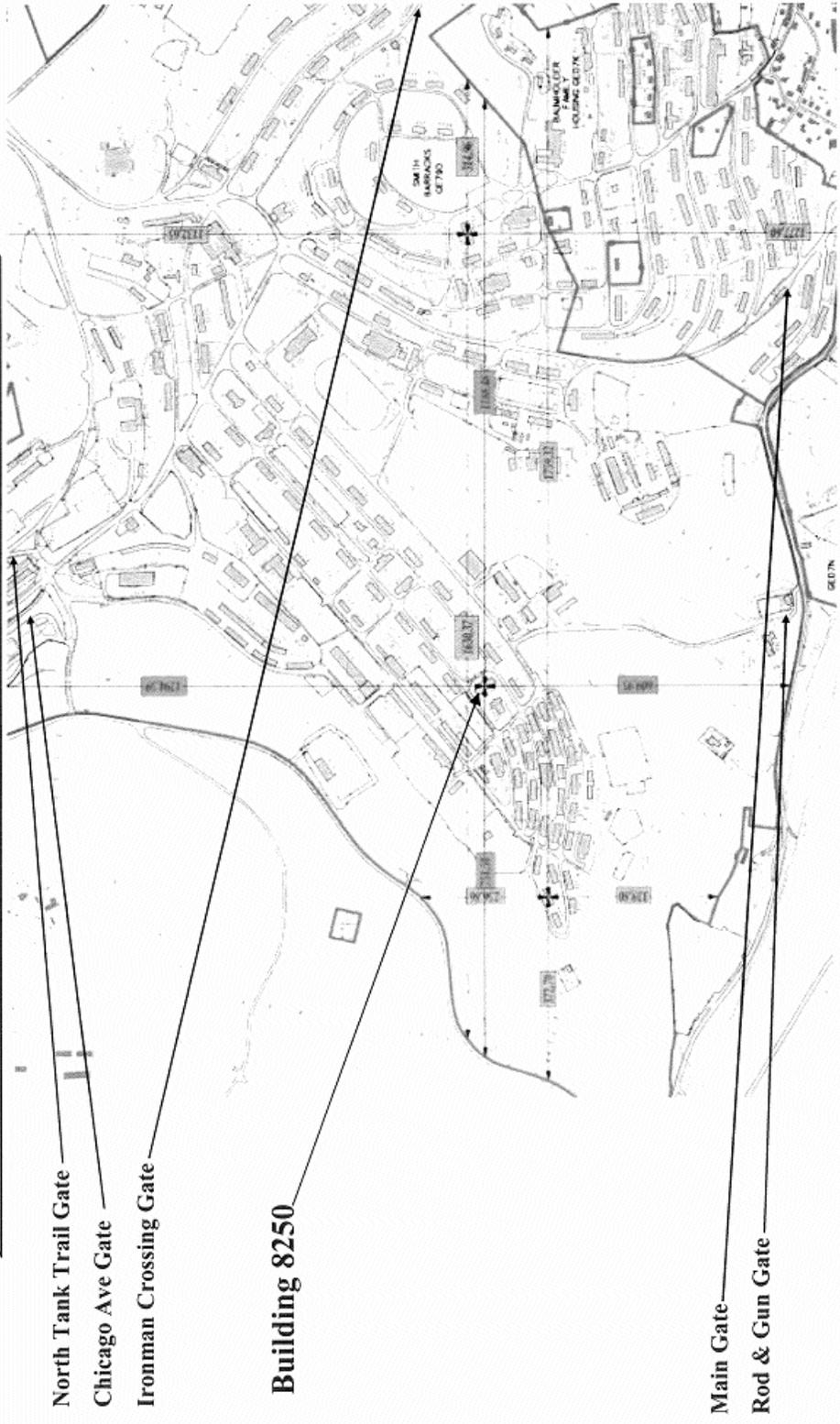


Bldg 8250 has 1 floor. We have no windows in the secure area. No local nationals work in the building.

What is Inspectable Space (IS)?
 The Three-Dimensional space surrounding equipment that
 process classified and/or sensitive information.
 Diagrams shown below are samples of information
 TEMPEST needs to determine IS.



KASERNE / INSTALLATION MAP



Bldg 8250 is located .5 miles from main gate

AE Form 380-85B is marked FOR OFFICIAL USE ONLY. The information shown in the sample below is generic, Unclassified, and provided for demonstration purposes only.

UNCLASSIFIED//FOR OFFICIAL USE ONLY Army Facility/System TEMPEST Questionnaire (AE Reg 380-85)		
This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption 1 applies.		
Part I - Miscellaneous		
1. Name of requester 1LT Jonathan Morales	2. Telephone number 337-1111	3. Fax 337-2222
4. Unit/facility mail address and e-mail 50th Transportation Battalion Building 2000 Unit 00111 APO AE 09000-9111	5. Facility POC 1LT Jonathan Morales	6. SCIF number <input checked="" type="checkbox"/> NA
Part II - General Information		
Select the best answer for each question.		
1. Facility (select one)	<input type="checkbox"/> Mobile	<input checked="" type="checkbox"/> *Fixed (*stays in one place more than 60 days).
2. System/equipment authorized in (select one)	<input checked="" type="checkbox"/> Garrison	<input type="checkbox"/> Field <input type="checkbox"/> Both
3. Is this a tactical system? (select one)	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
3a. Type of evaluation? (select one)	<input checked="" type="checkbox"/> Garrison	<input type="checkbox"/> Field evaluation
4. Is the facility system located within the United States, its trust territories, or protectorates?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No <input type="checkbox"/> NA
5. Is the facility/system on a U.S. military post, camp, or station?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> NA
6. Is the building Government-owned or -leased?	<input type="checkbox"/> Government-owned	<input checked="" type="checkbox"/> Government-leased <input type="checkbox"/> NA
7. Is the facility Government-owned or -leased?	<input type="checkbox"/> Government-owned	<input checked="" type="checkbox"/> Government-leased <input type="checkbox"/> NA
8. Is the facility totally occupied by U.S. personnel?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> NA
9. Do foreign nationals have access to the facility?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> NA
10. Closet foreign nationals/non-Government personnel.	15 meters _____ meters	
10a. Do they share a common wall with the secure processing area?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No <input type="checkbox"/> NA
11. Is the power filtered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input checked="" type="checkbox"/> UNK
12. Is the equipment powered by a UPS (Uninterruptible Power System)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input checked="" type="checkbox"/> UNK
13. Does the facility/organization control access to power?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> UNK
14. Does the facility/organization control access to the telephone distribution room system?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> UNK
15. Does the facility/building have cable TV?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No <input type="checkbox"/> UNK
16. Where is the cable TV antenna located?	<input type="checkbox"/> UNK	
17. Is there a digital copier or fax machine with a hard diskdrive in the facility?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No <input type="checkbox"/> UNK
17a. Is the hard diskdrive in the digital copier or fax machine removable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No <input checked="" type="checkbox"/> UNK
Part III - Volume, Sensitivity, and Perishability of Information Processed (daily average calculated over a 30 day period).		
18. TS Special Category		
Unclassified	0	%
Secret Special Category	10	%
Secret Collateral	50	%
Confidential Special Category	5	%
Confidential Collateral	5	%
NOTE: The information in 18 above is the same as the information on DA Form 7483		
19. Average number of hours that the system processes information regardless of classification.	40	hrs
20. Is the bulk (51% or more) of the information being processed of long-term (strategic) or short-term (tactical) value?	<input type="checkbox"/> Long-term	<input checked="" type="checkbox"/> Short-term

AE FORM 380-85B, DATE

UNCLASSIFIED//FOR OFFICIAL USE ONLY

AE Form 380-85B is marked FOR OFFICIAL USE ONLY. The information shown in the sample below is generic, Unclassified, and provided for demonstration purposes only.

Part IV - Transmitter Questions	
21. Is there a transmitter located within 30 meters of the facility? (This includes, but is not limited to any wireless communications devices, such as keyboards and LANs.) NOTE: If NO, skip to question 26.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> UNK
22. How often is transmitter used?	___ hours/day ___ hours/week
23. Size of transmitter (power output)	___ Watts
24. What kind of antenna?	<input type="checkbox"/> Dish <input type="checkbox"/> Long/Wire <input type="checkbox"/> LPA <input type="checkbox"/> Whip <input type="checkbox"/> Other
25. What is the frequency range?	<input type="checkbox"/> HF <input type="checkbox"/> UHF <input type="checkbox"/> SHF <input type="checkbox"/> Microwave <input type="checkbox"/> Other
26. Is there a fire alarm system?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> UNK
27. What is the fire alarm system?	<input checked="" type="checkbox"/> Active <input type="checkbox"/> Passive <input type="checkbox"/> UNK (transmitter polling)
28. Are security guards on duty?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> UNK
29. Are the guards armed?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> UNK
30. Are random roving patrols conducted?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> UNK
Part V - Physical Security Questions	
31. Enclose the following items if they apply to the system/facility:	
a. Overhead maps/drawings of facility.	
(1) Outline within building the secure processing area. Include square footage of processing room and all adjacent rooms to the processing room.	
(2) Give the distance (in meters) from secure area boundary to facility outside walls.	
b. List of information-processing equipment to be used.	
(1) Manufacturer <u>SYSTEMATIC</u>	
(2) Model <u>Venture 50</u>	
(3) Type <u>PC</u>	
c. System wiring and rack evaluation drawings.	
32. Return completed form to:	
HQ USAREUR/7A (AEAGB-SAD-S) Unit 29351 APO AE 09014-9351	
33. Remarks	
34. Requester Signature	35. Date

AE FORM 380-85B, DATE (Back)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

GLOSSARY

SECTION I ABBREVIATIONS

66th MI Gp	66th Military Intelligence Group
AE	Army in Europe
AOR	area of responsibility
AR	Army regulation
BENELUX	Belgium, the Netherlands, Luxembourg
C-SIGINT	counter-signals intelligence
CB	citizens band
CI	counterintelligence
CTTA	certified TEMPEST technical authority
DA	Department of the Army
DMS	Defense Messaging System
DOD	Department of Defense
DSN	Defense Switch Network
DV	distinguished visitor
FTTA	facility technical threat assessment
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HF	high frequency
hrs	hours
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
ID	identification
INSCOM	United States Army Intelligence and Security Command
LMR	low-to-medium range
NA	not applicable
OPSEC	operations security
POC	point of contact
RF	radio frequency
SCIF	sensitive compartmented information facility
SHF	superhigh frequency
SIGINT	signals intelligence
SIGSEC	signals security
STE	secure telephone equipment
STU-III	secure telephone unit, third generation
TCC	telecommunications center
TCI	technical counterintelligence
TCR	TEMPEST countermeasures review
TSCM	technical surveillance countermeasures
TSCIF	temporary sensitive compartmented information facility
UHF	ultra high frequency
UNK	unknown
USAREUR	United States Army, Europe
VHF	very high frequency

SECTION II TERMS

after-duty-hour inspection

An unannounced check, known only to selected persons, and conducted after normal duty hours. This check determines whether or not the installation or office is complying with requirements for the physical protection of classified defense information. Inspectors conducting such checks should do so only with an escort from the installation or office concerned.

announced inspection

An inspection of which the installation or office to be inspected is aware. Personnel know the scheduled date of an announced inspection and can make necessary preparations.

counterintelligence advice and assistance visit

An informal service of limited scope provided by the supporting counterintelligence unit to help an office or unit identify and solve security problems and determine if it is complying with established security policy and procedures. Formal reports usually are not made. Assistance varies in scope. The service will not be requested to help prepare for another formal inspection (for example, annual general inspection, command inspection). Units will request advice and assistance services directly from the local counterintelligence element.

counterintelligence inspection

A service performed to determine compliance with established information security policy and procedures.

unannounced inspection

An inspection designed to determine if an installation or office is complying with existing requirements when special preparations have not been made. Only selected persons know of unannounced inspections in advance.