Headquarters
United States Army, Europe, and Seventh Army
Unit 29351
APO AE 09014
6 June 1996

USAREUR Regulation 380-85

Change 1

Security

Counterintelligence Services

For the Commander in Chief:

DAVID L. BENTON III
Major General, GS
Chief of Staff

Official:

ROBERT L. NABORS
Brigadier General, GS
Deputy Chief of Staff,
Information Management

Summary. This change—

a. Provides updated unit designations, office symbols, and addresses for the 66th Military Intelligence Group (Provisional) and the Collection Battalion.

b. Provides an updated index of USAREUR counterintelligence offices.

Suggested Improvements. The proponent of this change is the Office of the Deputy Chief of Staff, Intelligence, HQ USAREUR/7A (AEAGB-CI-S, 370-6564/8179). Users may send suggestions to improve this change on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander in Chief, USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014.

Distribution. Distribute according to DA Form 12-88-E, block 0380, command level B.

1. USAREUR Regulation 380-85, 3 May 1994, is changed as follows:

Throughout. Change "66th Military Intelligence Brigade" and "66th MI Bde" to "66th Military Intelligence Group (Provisional)" and "66th MI Gp (Prov)".

Throughout. Change "18th Military Intelligence Battalion" and "18th MI Bn" to "Collection Battalion" and "Collection Bn".

Throughout. Change "66th MI Bde, ATTN: IAPGE-OR, CMR 456, APO AE 09157" to "66th MI Gp, ATTN: IAPG-OP, Unit 25009, APO AE 09178".

Throughout. Change "Detachment B, Company A, 18th Military Intelligence Battalion, ATTN: IAGPE-GI-TE,CMR 456, APO AE 09157" to "Collection Battalion, ATTN: IAPG-VOT-T, Unit 25009, APO AE 09178".

Throughout. Change "CDR 66TH MI BDE AUGSBURG GE//IAGPE-OR//" to "CDR 66TH MI GP AUGSBURG GE//IAPG-OP//".

Throughout. Change "CDR 18TH MI BN AUGSBURG GE//IAGPE-GI-TE//" to "CDR COLLECTION BN AUGSBURG GE//IAPG-VOT-T//".

Page A-1, paragraph A-4a. Change "USAREUR Regulation 190-3, Installation Access" to "USAREUR Regulation 190-13, The USAREUR Physical Security Program".

Page B-2, paragraph B-3k. In line 4, change "CDR 66TH MI BDE AUGSBURG GE//IAGPE-OS-S//" to "CDR 66TH MI GP AUGSBURG GE//IAPG-OR//".

Page C-1. Supersede tables C-1 and C-2 as follows:

Table C-1
V Corps Counterintelligence Offices

Locations	Military Telephone Numbers	Civilian Telephone Numbers
Bad Kreuznach FO	490-6056/6084/6085	0671-609-6056/6084/6085
Baumholder FO	485-6209/7339/7434	06783-6-6209/7339/7434
Hanau FO	322-8697/8816	06181-88-8697/8816
Schwetzingen FO	379-6019/6125/7637	06202-80-6019/6125/7637
Wiesbaden FO	337-6377/6381	0611-705-6377/6381
Würzburg (1st Infantry Division FO)	350-6765/7192	0931-889-6765/7192

Table C-2
66th Military Intelligence Group Counterintelligence Offices

Locations	Military Telephone Numbers	Civilian Telephone Numbers
Augsburg, GE (MID)	435-6151/7420	0821-540-6151/7420
Chièvres, BE (BENELUX RO)	361-5408/5539	0032-68-27-5408/5539
Grafenwöhr, GE (RO)	475-6241/7105	09641-83-6241/7105
Hohenfels, GE (RO)	466-4682	09472-83-4682
Kaiserslautern, GE (MID)	489-6503/6528/7080	0631-536-6503/6528/7080
Livorno, IT (584th MID)	633-7777/7778	0039-050-54-7777/7778
Maastricht, NL (BENELUX MID)	360-4292	0031-43-328-4471
Schwetzingen, GE (MID)	379-6035/6231/6249	06202-80-6035/6231/6249
Stuttgart, GE (MID)	421-2206/2208/2209	0711-544158
Vicenza, IT (584th MID)	634-7681/7688/8030	39-444-51-7681/7688/8030
Würzburg, GE (MID)	351-4113/4217/4317	0931-296-4113/4217/4317

2. Post these changes per DA Pamphlet 310-13.

3. File this change in front of the regulation for reference.

Headquarters
United States Army, Europe, and Seventh Army
Unit 29351
APO AE 09014
3 May 1994

***USAREUR Regulation 380-85**

Security

Counterintelligence Services

For the Commander in Chief:

CRAIG A. HAGAN
Major General, GS
Chief of Staff

Official:

CHARLES G. SUTTEN, JR.
Brigadier General, GS
Deputy Chief of Staff,
Information Management

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

Applicability. This regulation applies to—

a. USAREUR organizations and activities.

b. Organizations supported by USAREUR.

Supplementation. Commanders will not supplement this regulation without Commander in Chief, USAREUR (AEAGB-CI-S), approval.

Interim Changes. Interim changes to this regulation are not official unless authenticated by the Deputy Chief of Staff, Information Management, USAREUR. Interim changes will be destroyed on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent of this regulation is the Office of the Deputy Chief of Staff, Intelligence, HQ USAREUR/7A (AEAGB-CI-S, 370-6564/8179). Users may send suggestions to improve this regulation on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander in Chief, USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014.

Distribution. Distribute according to DA Form 12-88-E, block 0380, command level B.

1. PURPOSE

This regulation—

a. Describes counterintelligence (CI) services in USAREUR.

b. Prescribes policy and procedures for requesting CI services.

c. Does not apply to providing physical security services. Physical security is a responsibility of the Provost Marshal, USAREUR. Exceptions to this policy apply to protect—

(1) Classified information from being compromised.

(2) Information from technical surveillance.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary explains abbreviations and terms used in this regulation.

4. RESPONSIBILITIES

a. The Deputy Chief of Staff, Intelligence (DCSINT), USAREUR (AEAGB-CI-S), will—

(1) Establish—

(a) A CI services program in USAREUR.

(b) Policy for CI services.

(2) Coordinate requests for CI services from HQ USAREUR/7A staff offices; USAREUR major, separate major, and assigned commands (USAREUR Reg 10-5); and attached or supported units.

***This regulation supersedes USAREUR Regulation 380-85, 7 April 1988.**

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

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

(5) Direct requests for CI services.

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

b. The Commander, 66th Military Intelligence Brigade (66th MI Bde), provides CI service support to HQ USAREUR/7A staff offices; USAREUR major, separate major, and assigned commands; and attached or supported units.

c. The Commander, V Corps, will provide CI services to corps and corps-supported units using assigned CI assets.

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

(2) When the requirements for CI services to corps units exceed the capability of assigned CI assets, the Commander, V Corps, may request additional support from the Commander in Chief, USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014. An information copy of the request will be sent to Commander, 66th MI Bde, ATTN: IAGPE-OR, CMR 456, APO AE 09157.

5. POLICY

a. The DCSINT is the proponent for CI services in USAREUR. Security managers will identify the need for CI services and send requests to appropriate commanders. Commanders of supported units will—

(1) Consolidate CI needs.

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

(a) Should be in order of priority.

(b) Is due 1 February each year to Commander in Chief, USAREUR, with an information copy sent to the Commander, 66th MI Bde (para 4c(2) provides addresses).

b. CI advice and assistance may be informal and responsive to the needs of the requesting unit. Units may request advice from the supporting CI 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 maintain results of inspections for reference during future CI 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 CI SERVICES

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

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

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

b. Security managers will send time-sensitive requests (requests for service in less than 45 days) for 66th MI Bde CI services by message to CINCUSAREUR HEIDELBERG GE//AEAGB-CI-S// and CDR 66TH MI BDE AUGSBURG GE//IAGPE-OR//. Intermediate commands will be information addressees. These requests will tell when the service is needed and include a justification. This procedure will not be used to avoid normal requesting procedures. The requesting activity will fund unscheduled and unprogrammed requests for TSCM services. Requirements for other non-scheduled services are established in this regulation (para 13c) and in the publications in appendix A.

c. The DCSINT, in coordination with the Commander, 66th MI Bde, will approve or disapprove requests.

d. Appendix B explains procedures for requesting TSCM services.

e. AR 380-19-1 provides TEMPEST policy, responsibilities, and assessment requirements to control compromising emanations. Paragraph 13 explains TEMPEST services.

f. Field Manual 34-60 describes counter-SIGINT. Paragraph 12 and USAREUR Regulation 380-53 explain counter-SIGINT services.

g. Appendix C lists locations and telephone numbers of V Corps and 66th MI Bde CI offices. Units may contact these offices for information on available CI support.

h. Requests for services covered by this regulation will be classified according to this regulation, appendix B; Director of Central Intelligence Directive 1/21; AR 380-5; AR 380-40; AR 380-53; AR 381-14; AR 380-19, AR 380-19-1, AR 381-20; other derivative authority (AR 380-5); and the sensitivity of the information in the request.

7. COORDINATION

a. Units that send CI service requests to USAREUR will include the name, rank, location, and telephone number of the unit point of contact (POC). After the request has been validated by the DCSINT (AEAGB-CI-S), the 66th MI Bde supporting element will—

(1) Coordinate with the POC.

(2) Determine the scope of services to be provided and ensure resources are available.

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

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

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

(1) Refused access to material or entry to areas.

(2) Unduly delayed.

8. SECURITY VIOLATIONS AND DEFICIENCIES

a. Persons conducting CI services will report possible losses or compromises of classified material according to AR 380-5 and USAREUR Supplement 1, AR 380-40, or AR 381-14, as applicable.

b. When military intelligence personnel have determined the possible loss or compromise of classified information during a CI service, the CI service report will include the possible loss or compromise as a finding and indicate an appropriate recommendation.

9. REPORTS

a. Paragraph 11 and appendix B prescribe formats, suspenses, and distribution requirements for TSCM reports.

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

c. Classified inspection reports, when required, will be marked according to AR 380-5 and USAREUR Supplement 1.

10. CI SCHEDULES FOR INSPECTION

a. After an initial service, TSCM services will be scheduled on a recurring basis, when required.

b. Other CI services (such as counter-SIGINT and TEMPEST services) are scheduled as required, based on requests.

11. CORRECTIVE ACTIONS

a. The Commander, V Corps, will send reports of corrective action taken on CI services conducted under paragraph 4c to Commander in Chief, USAREUR (para 4c(2) provides the address).

b. Reports requiring corrective actions resulting from TEMPEST, TSCM, and CI inspections will be endorsed through command channels to the Commander in Chief, USAREUR, with an information copy sent to the Commander, 66th MI Bde (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 corrective actions taken.

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

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

12. COUNTER-SIGNALS INTELLIGENCE SERVICES

a. Counter-SIGINT distinguishes between signals security (SIGSEC) and counterintelligence activities that support SIGSEC. Counter-SIGINT is intelligence support for a command's SIGSEC program. Counter-SIGINT has the following support functions:

(1) Countermeasures evaluation.

(2) Countermeasures recommendations.

(3) Threat assessment.

(4) Vulnerability and possible-risk assessment.

b. Communications security monitoring may be included in the counter-SIGINT process during the evaluation phase (USAREUR Reg 380-53).

c. USAREUR Regulation 380-53 provides procedures for requesting counter-SIGINT services.

13. TEMPEST SERVICES

a. TEMPEST Inspection.

(1) A TEMPEST inspection will be conducted at facilities that electrically process classified information. The inspection is a desktop review of the facility TEMPEST assessment/risk analysis (FTA/RA).

(2) The FTA/RA will be completed according to AR 380-19-1, chapter 3. Preparation of the FTA/RA is required for commanders who establish or plan to alter, expand, or relocate facilities or systems to process classified information electrically.

(3) Unit security personnel will send completed FTA/RA to the United States Army Intelligence and Security Command (INSCOM) support element, Detachment B, Company A, 18th Military Intelligence Battalion, ATTN: IAGPE-GI-TE, CMR 456, APO AE 09157.

(4) Based on a review of the FTA/RA, the Commander, Detachment (Det) B, Company (Co) A, 18th Military Intelligence Battalion (18th MI Bn), will provide a memorandum of concurrence or nonconcurrence and recommend countermeasures, if appropriate. Additional TEMPEST support, if required (for example, on-site inspection, verification, or TEMPEST-instrumented test), will be scheduled by the INSCOM support element, in coordination with the supported command.

(5) Activities may request telephone advice in completing the FTA/RA from the Commander, Detachment B, Company A, 18th MI Bn (DSN/STU-III 434-7515).

b. 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) Review of the FTA/RA.

(3) Facility or system vulnerability and sensitivity.

c. Unscheduled TEMPEST Support. Units with a compelling need and strong justification may request unscheduled TEMPEST support for review and validation. Requests will be sent through the command TEMPEST control officer to the Commander in Chief USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014. Information copies will be sent to the Commander, 66th MI Bde, ATTN: IAGPE-OR, CMR 456, APO AE 09157; the Commander, Detachment B, Company A, 18th MI Bn, ATTN: IAGPE-GI-TE, CMR 456, APO AE 09157; and to the appropriate persons in the chain of command.

(1) The requesting unit will fund unprogrammed TEMPEST support. Requests for such support will include a fund citation to defray temporary duty expenses.

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

(a) Dates and results of previous services.

(b) Facility or system to be inspected.

(c) Justification and urgency of need.

(d) Point of contact (local TEMPEST coordination officer, information system security officer, information system security manager).

(e) Description of service needed.

(3) Once validated by the DCSINT (AEAGB-CI-S), requests for unprogrammed TEMPEST support will be arranged by priority, based on the requesting activity's need.

Appendixes

Glossary

APPENDIX A
REFERENCES

A-1. DIRECTOR CENTRAL INTELLIGENCE DIRECTIVE

Director Central Intelligence Directive 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities. (This publication is available through the Office of the Deputy Chief of Staff, Intelligence, HQ USAREUR/7A (AEAGB-CI-S).)

A-2. ARMY REGULATIONS

a. AR 25-55, The Department of the Army Freedom of Information Act Program.

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

c. AR 380-19, Information Systems Security.

d. AR 380-19-1, (C) Control of Compromising Emanations (U).

e. AR 380-28, (C) Department of the Army Special Security System (U).

f. AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material.

g. AR 380-53, Communications Security Monitoring.

h. AR 381-14, (S) Technical Surveillance Countermeasures (TSCM) (U).

i. AR 381-20, US Army Counterintelligence Activities.

j. AR 530-1, Operations Security (OPSEC).

A-3. FIELD MANUAL

Field Manual 34-60, Counterintelligence.

A-4. USAREUR REGULATIONS

a. USAREUR Regulation 190-3, Installation Access.

b. USAREUR Regulation 380-19, Information Systems Security.

c. USAREUR Regulation 380-40, Safeguarding and Controlling Communications Security Material.

d. USAREUR Regulation 380-53, Counter-Signals Intelligence Support.

APPENDIX B
COUNTERINTELLIGENCE TECHNICAL SURVEILLANCE COUNTERMEASURES

B-1. PURPOSE
This appendix prescribes policy and procedures for requesting and classifying counterintelligence (CI) technical surveillance countermeasures (TSCM) services in USAREUR.

B-2. POLICY
The USAREUR TSCM program includes measures taken to reduce USAREUR's vulnerability to technical surveillance threats.

a. Secure facilities should be used for classified discussions.

(1) A secure facility is an area that—

(a) Complies with AR 381-14 security standards.

(b) Has received TSCM services.

(c) Corrects deficiencies.

(2) AR 380-5, paragraph 5-205, and this appendix, paragraph B-3a, provide procedures for ensuring security during meetings and conferences.

b. Plans for constructing or modifying sensitive areas will incorporate physical and technical security standards established in AR 381-14. The organization constructing or modifying a sensitive area should arrange a TSCM preconstruction service early in the planning cycle.

c. To protect the validity of TSCM services in the serviced areas, references to requesting, planning, and conducting TSCM services will be in writing and classified Secret. These services will not be discussed until they are completed.

B-3. PROCEDURES

a. Classified briefings or discussions often have to be conducted at a location that has not had a TSCM survey (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—

(1) 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, or facilities generally open to the public will be avoided.

(2) Control access to the entire physical perimeter of the facility, including ceilings, floor, and walls. Guards should—

(a) Be present during classified discussions.

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

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

(3) 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.

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

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

b. A TSCM service is—

(1) Often referred to as a "tech sweep" or a "debugging."

(2) Conducted to detect devices covertly installed to monitor an area by audible or visual means.

(3) Preventive, because compliance with the service will make it more difficult to install covert devices.

(4) Time-consuming. TSCM services involve a physical search and use of technical equipment. TSCM services impose some requirements on the requester (for example, the requester must ensure the serviced area remains protected from unauthorized visitors).

c. Before requesting a TSCM service, the commander should consider the following information:

(1) The passage of time is not justification for repeating a TSCM service. The limited technical service assets in USAREUR require that TSCM services be—

(a) Conducted selectively.

(b) Based on a valid need for the service (for example, foreign national employees or contractors having renovated a facility, relocation of a facility that had an authorized TSCM service, indications that concealed audio or visual surveillance is present).

(2) The area serviced—

(a) Should have been declared a restricted area (USAREUR Reg 190-3) by the commander of the organization.

(b) Will be used regularly to discuss sensitive information (AR 381-14).

(3) The TSCM service immediately will lose its validity under certain conditions (AR 381-14). The requester must be prepared at the beginning of the survey to—

(a) Maintain continuous and effective control over the searched area.

(b) Provide escorts for persons who need occasional access to the facility but who do not meet the criteria for unescorted access.

(c) Prevent repairs or alterations to or in sensitive areas, except under the supervision of qualified and responsible personnel who can control the workers.

(d) Prevent the introduction of new furnishings that have not been inspected thoroughly by the most qualified security or technical maintenance personnel available.

(e) Ensure the TSCM team is not unduly delayed and has unrestricted access in and around the areas to be serviced.

d. A limited TSCM service may be conducted on a one-time basis if sensitive material will be discussed. Normally, the service is done the day of the classified discussion. The security precautions in a above will apply. The service will become invalid immediately after the facility is used.

e. Units will send requests for TSCM services through command channels to the Commander in Chief, USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014. A copy will be sent to the Commander, 66th Military Intelligence Brigade, ATTN: IAGPE-OR, CMR 456, APO AE 09157, and the Commander, 18th Military Intelligence Battalion, ATTN: IAGPE-GI-TE, CMR 456, APO AE 09157. Requests may be sent by electrical message to CINCUSAREUR HEIDELBERG GE//AEAGB-CI-S//. An information copy will be sent to CDR 66TH MI BDE AUGSBURG GE//IAGPE-OR//, CDR 18TH MI BN// AUGSBURG GE//IAGPE-GI-TE//, and intermediate headquarters.

f. Requests for TSCM services will—

(1) Be classified at least Secret (para B-4).

(2) State—

(a) The specific area to be serviced, including the office or activity occupying the facility, room number, building number or name, street, post or installation, city, state, country, and zip code or Army post office number.

(b) The primary use of the area to be serviced.

(c) The size of the area in number of square feet of floor space.

(d) The number of telephones installed in the area, by type (for example, single-line, multi-line, call-director) and model number. This information normally is printed on the bottom of each telephone.

(e) The name, position title, and secure telephone number of the person who has security responsibility for the area or who will act as the point of contact for the TSCM team during the service.

(f) Whether or not special access authorizations are required for TSCM personnel conducting the service. (TSCM special agents have Top Secret security clearances.)

(g) The sensitivity and classification of the information discussed and processed in the area and the frequency of discussion or processing (for example, daily, weekly, monthly).

(h) Actions taken to correct previously noted security vulnerabilities or deficiencies. Requests for areas previously provided TSCM service will include a justification for another survey.

(3) Give the date or period for which the service will be needed, if applicable, and a statement that—

(a) Construction is or will be completed by the time the TSCM service is provided.

(b) Equipment and furnishings are or will be in place by the time the TSCM service is provided.

(c) Adequate physical security measures are or will be in place to keep unauthorized personnel from entering during and after the service. The requester will provide a brief description of the security controls.

(4) Describe unique mission responsibilities that would affect the priority to be assigned to the TSCM service.

g. After an area has received a TSCM service, no additional services will be performed unless—

(1) Previously identified security vulnerabilities are corrected.

(2) One of the following actions occurs:

(a) Construction was done in the area by persons without clearances.

(b) The United States Army Intelligence and Security Command has approved the area for recurring TSCM service (AR 381-14).

(c) Unauthorized personnel have had uncontrolled or unescorted access to the area.

h. 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.

i. For operations security reasons, TSCM services and surveys will be unannounced.

j. The requesting unit will fund unprogrammed requests (requests not identified to the Deputy Chief of Staff, Intelligence, USAREUR (AEAGB-CI-S), by 1 February of each year according to basic reg, para 5a(2)(b)) for TSCM inspections and survey. Requests for such services will include a fund cite to defray temporary duty expenses.

k. The discovery of suspected technical surveillance devices will be reported to the supporting 66th Military Intelligence Brigade CI element by immediate Secret message to CDR 66TH MI BDE AUGSBURG GE//IAGPE-OS-S//. An information copy will be sent to CDR 18TH MI BN AUGSBURG GE//IAGPE-GI-TE//. Personnel will not tamper with the device, significantly change activity in the area, or discuss any aspect of the device until contacted by trained TSCM personnel.

B-4. CLASSIFICATION

a. Requests for TSCM services will be classified Secret and marked as follows:

Classified by: AR 381-14, paragraph 3-14e.

Downgrade to: Confidential on completion of service.

Declassify on: Originating agency's determination required.

b. TSCM personnel will not honor requests received through nonsecure means.

c. Requesters will send information about the TSCM service to persons who require the information. Persons will not discuss a service that is planned or in progress while in the area being serviced. Under certain conditions, such conversation may cause termination of the service.

B-5. REPORTS

The servicing team will give the original TSCM report to the serviced unit and send a copy to the Commander in Chief, USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014. The unit will complete corrective actions based on AR 381-14, paragraph 10.

APPENDIX C
COUNTERINTELLIGENCE OFFICES

Table C-1 provides locations and telephone numbers of V Corps counterintelligence offices. Table C-2 provides locations and telephone numbers of 66th Military Intelligence Brigade, 18th Military Intelligence Battalion, counterintelligence offices. The glossary explains abbreviations used.

Table C-1
V Corps Counterintelligence Offices

Locations	Military Telephone Numbers	Civilian Telephone Numbers
Ansbach (165 MI Bn RO)	468-7692/7837	06981-183-7692/7837
Bad Kreuznach (1st AD FO)	490-6056/6084/6085	0671-609-6056/6084/6085
Baumholder FO	485-6209/7339/7434	06783-6-6209/7339/7434
Darmstadt FO	348-6630	06151-69-6630
Frankfurt FO	325-8900/8901	069-1541-8900/8901
Frankfurt (Abrams FO)	320-6456/8056	069-151-6456/8056
Friedberg FO	324-3083/3458	06031-81-3083/3458
Hanau FO	322-8816	06181-88-8816
Kitzingen DO	355-2440	09321-702-2440
Nürnberg FO	460-6324/6483	0911-700-6324/6483
Schweinfurt DO	354-6876	09721-96-6876
Wiesbaden FO	337-6377/6381	0611-705-6377/6381
Würzburg (3d Infantry Division FO)	350-7192	0931-889-7192

Table C-2
66th Military Intelligence Brigade, 18th Military Intelligence Battalion, Counterintelligence Offices

Locations	Military Telephone Numbers	Civilian Telephone Numbers
Augsburg, GE (MID)	434-6151/7420	0821-448-6151/7420
Bad Aibling, GE (RO)	441-3700	08061-38-3700
Berlin (766th MID)	332-6228/6828	030-819-6228/6828
Chievres, BE (BENELUX MID)	361-5223/5539	0032-68-27-5223/5539
Darmstadt, GE (RO)	348-6677/7356	06151-64266
Frankfurt, GE (MID)	325-7620/8359	069-1541-7620/8359
Giessen, GE (RO)	343-6598/8377	0641-42078
Grafenwöhr, GE (RO)	475-6241/7105	09641-83-6241/7105
Heidelberg, GE (MID)	370-6414/6910/8049	06221-390678
Kaiserslautern, GE (MID)	489-6503/6528/7080	0631-536-6503/6528/7080
Karlsruhe, GE (RO)	376-6288/7389	0721-73504
Livorno, IT (584th MID)	633-7777/7778	39-050-54-7777/7778
Maastricht, NL (RO)	360-4471/4478	0432844332-4426
Mainz, GE (RO)	334-8350/8479	06131-48-8350/8479
Mannheim, GE (RO)	380-8270/8276	0621-730-8270/8276
Nürnberg, GE (MID)	460-7070/7137/7609	0911-700-7070/7137/7609
Pirmasens, GE (RO)	495-7329/7332	06331-63820
Stuttgart, GE (MID)	421-2208/2209	0711-544158
Vicenza, IT (584th MID)	634-7687/7688	39-444-51-7687/7688
Würzburg, GE (MID)	350-621/6407	0931-8899-6217/6407

GLOSSARY

SECTION I
ABBREVIATIONS

1st AD	1st Armored Division
18th MI Bn	18th Military Intelligence Battalion
66th MI Bde	66th Military Intelligence Brigade
AR	Army regulation
BE	Belgium
BENELUX	Belgium, The Netherlands, Luxembourg
CI	counterintelligence
counter-SIGINT	counter-signals intelligence
DCSINT	Deputy Chief of Staff, Intelligence, USAREUR
DO	day office
DOD	Department of Defense
FO	field office
FTA/RA	facility TEMPEST assessment/risk analysis
GE	Germany
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
INSCOM	United States Army Intelligence and Security Command
IT	Italy
MID	military intelligence detachment
NL	The Netherlands
POC	point of contact
RO	resident office
SIGSEC	signals security
TSCM	technical surveillance countermeasures
USAREUR	United States Army, Europe

SECTION II
TERMS

after-duty-hour inspection
An unannounced check, known only to selected persons, 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 that the installation or office to be inspected is aware of. Personnel know the scheduled date of announced inspection and can make necessary preparations.

counterintelligence advice and assistance visit
An informal service of limited scope provided by the supporting counterintelligence unit. The visit will help an office or unit identify and solve security problems and determine compliance 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 installation or office compliance with existing requirements when special preparations have not been made. Only selected persons know of an unannounced inspections in advance.