Army Regulation 381–10

Military Intelligence

US Army Intelligence Activities

Headquarters
Department of the Army
Washington, DC
1 July 1984

Unclassified

SUMMARY of CHANGE

AR 381-10
US Army Intelligence Activities

RESERVED

FOREWORD

This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect United States persons It implements DoD Directive 5240 1, and replaces the November 30, 1979 version of DoD Regulation 5240 1–R It is applicable to all DoD intelligence components

Executive Order 12333, "United States Intelligence Activities," stipulates that certain activities of intelligence components that affect US persons be governed by procedures issued by the agency head and approved by the Attorney General Specifically, procedures 1 through 10, as well as appendix A, herein, require approval by the Attorney General Procedures 11 through 15, while not requiring approval by the Attorney General, contain further guidance to DoD Components in implementing Executive Order 12333 as well as Executive Order 12334, "President's Intelligence Oversight Board "

Accordingly, by this memorandum, these procedures are approved for use within the Department of Defense Heads of DoD components shall issue such implementing instructions as may be necessary for the conduct of authorized functions in a manner consistent with the procedures set forth herein

This regulation is effective immediately

(Signed) 10/4/82
William French Smith
Attorney General of the
United States

Signed 12/7/82
Caspar W Weinberger
Secretary of Defense

Headquarters
Department of the Army
Washington, DC
1 July 1984

*Army Regulation 381–10

Effective 1 August 1984

Military Intelligence

US Army Intelligence Activities

By Order of the Secretary of the Army.

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

Official.

ROBERT M. JOYCE
Major General, United States Army
The Adjutant General

History

Summary This regulation, which sets forth policies and procedures governing the conduct of intelligence activities by Department of the Army intelligence components has been revised This revision implements DoD Directive 5240 1 and DoD 5240 1–R which implement Executive Order 12333, United States Intelligence Activities It includes all of DoD 5240 1–R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," dated December 1982, and added implementing supplementing instructions where required These additions are set in boldface type

Applicability

1 This regulation applies to the following

a All Army intelligence components, as that term is defined in appendix A, paragraph 8

b Other military personnel and civilian employees of the Department of the Army when they engage in intelligence activities as that term is defined in appendix A, paragraphs 8 and 13

c Members of the Army National Guard and US Army Reserve when they are performing Federal duties or engaging in activities directly related to a Federal duty or mission

2 Army intelligence components are explicitly excluded from the provisions of AR 380–13

3 This regulation is not applicable to activities covered under Presidential Directive/National Security Council—9

Proponent and exception authority Not applicable

Impact on the New Manning System This regulation does not contain information that affects the New Manning System

Army management control process. Not applicable

Supplementation Supplementation of this regulation is prohibited unless prior approval is obtained from HQDA (DAMI–CIC), WASH DC 20310

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

Suggested Improvements. The proponent agency of this regulation is the Office of the Assistant Chief of Staff for Intelligence 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

Distribution Distribution To be distributed in accordance with DA Form 12–9A requirements for AR, Military Intelligence Active Army, B, ARNG and USAR, C

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 381–10, 15 February 1982

Unclassified

Contents—Continued

Part 1
PROCEDURE 1. GENERAL PROVISIONS

A. APPLICABILITY AND SCOPE

1 These procedures apply only to "DoD intelligence components," and other DA components performing "intelligence activities," as defined in Appendix A Procedures 2 through 4 provide the sole authority by which such components may collect, retain and disseminate information concerning United States persons Procedures 5 through 10 set forth applicable guidance with respect to the use of certain collection techniques to obtain information for foreign intelligence and counterintelligence purposes Authority to employ such techniques shall be limited to that necessary to perform functions assigned the DoD intelligence component concerned Information may be gathered by intelligence components using techniques described in procedures 5 through 10 for other then foreign intelligence or counterintelligence (CI) purposes However, such collection must comply with the following be based on a proper function assigned to the intelligence component, employ the least intrusive lawful investigative techniques reasonable available, and comply with the appropriate provisions of this regulation Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities

2 The function of DoD intelligence components not specifically addressed herein shall be carried out in accordance with applicable policy and procedure

3 These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components Involvement by an Army intelligence component in civil disturbance activities is governed by the Department of the Army (DA) Civil Disturbance Plan (Garden Plot) dated 3 August 1978 When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter tot the appropriate law enforcement agency in accordance with procedures 12 and 15, or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcement procedures If evidence surfaces during the course of an investigation by an Army intelligence component that provides reasonable belief that a crime has been committed and which under AR 195–2 also may be under the investigative jurisdiction of the US Army Criminal Investigation Command (USACIDC), details of the investigation will be provided to the USACIDC under AR 381–20

4 DoD intelligence components shall not request any person or entity to undertake any activity forbidden by Executive Order 12333, reference (a), or this regulation

B PURPOSE

The purpose of these procedures is to enable DoD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect United States person are carried out in a manner that protects the constitutional rights and privacy of such persons This regulation is intended to complement other intelligence regulatory policy, it does not establish independent authority for intelligence activities Therefore, activities and investigations described elsewhere, such as AR 381–12, AR 381–20, and Director of Central Intelligence Directives, must be conducted in accordance with these procedures For example, in determining whether an intelligence component may conducted an investigation that involves a US person, the component should first determine whether it has the mission and authority to conduct the type of investigation involved That determination is made utilizing applicable regulations, Director of Central Intelligence Directives, Defense Intelligence Agency guidance, and so forth Once that determination is made, and the component can establish its authority to conduct the investigation involved, this regulation, particularly Procedure 2, should be used to determine whether particular items of information about US persons may be collected during the conduct of the otherwise authorized investigation Intelligence components should be aware that number of concepts and terms commonly used within the intelligence community have unique definitions in this regulation For example, activities commonly considered part of a "CI investigation" (AR 381–20, appendix) may be considered "personnel security" matters under this regulation (See app A, secs 19 and 20)

C. INTERPRETATION

1 These procedures shall be interpreted in accordance with their stated purpose

2 All defined terms appear in appendix A Additional terms, not otherwise defined, are explained in the text of each procedure, as appropriate

3 All question of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned Intelligence component commanders will seek legal advice from their supporting judge advocates When questions cannot be resolved locally, they will be forwarded through command channels to HQDA (DAMI–CIC), WASH DC 20310, for coordination with the Office of The Judge Advocate General Questions that cannot be resolved in this manual shall be referred to the General Counsel of the Military Department concerned, or, as appropriate, the General Counsel of the Department of Defense for resolution

D EXCEPTIONS TO POLICY

Requests for exception to the policies and procedures established herein shall be made in writing to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense and, if required, the Attorney General for any such exceptions Request for exceptions to policy will be forwarded through command channels to HQDA (DAMI–CIC), WASH DC 20310

E AMENDMENT

Request for amendment of these procedures shall be made to the Deputy under the Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense, and, if required, the Attorney General, for any such amendment

F REQUESTS FOR APPROVAL

Requests to conduct any activity authorized by this regulation that requires HQDA or higher level approval (such as the Secretary of the Army or the US Attorney General) will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310 Complete justification must accompany each request

G GENERAL PROHIBITIONS

DA components will not conduct or provide support for the conduct of special activities, unless such actions have been approved by the President and directed by the Secretary of Defense Exceptions will be in time of war declared by the Congress or during a period covered by a report from the President and directed by the Secretary of Defense Under no circumstances will a DA employee engage in, or conspire to engage in, assassination

Part 2
PROCEDURES 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

A APPLICABILITY AND SCOPE

This procedures specifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques Nothing in this procedure will be interpreted as authorizing the collection of any information relating to a US person solely because of lawful advocacy of measures opposed to Government policy

B EXPLANATION OF UNDEFINED TERMS

1 Collection Information shall be considered as "collected" only when it has been received for use by an employee of a DoD

intelligence component in the course of his official duties For information to be "received for use" and therefore "collected" by an Army intelligence component, an employee must take some affirmative action that demonstrates an intent to use or retain the information received (such as production of a report, filing of an investigative summary, or electronic storage of received data) Establishment of "unofficial files" and the like may not be used to avoid the application of this procedure Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedures when an employee of such component officially accepts, in some manner, such information for use within that component Data acquired by electronic means is 'collected" only when it has been processed into intelligible form Information held, or forwarded to a supervisory authority, solely for the purpose of making a determination about the collectability of that information under this procedure (and not otherwise disseminated within the component) is not "collected"

2 Cooperating sources means person or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information, at the request of such components or on their own initiative Cooperating sources must be either informed or otherwise have knowledge that they are dealing with a DoD intelligence component These include government agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments

3 Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization, or person

4 Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that he is providing such information to the Department of Defense or a component thereof

C TYPES OF INFORMATION THAT MAY BE COLLECTED ABOUT UNITED STATES PERSONS

Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories Note Terms used in this part are defined in appendix A and may differ substantially from traditional Army usage

1 Information obtained with consent In may be collected about a United States person who consents to such collection

2 Publicly available information Information may be collected about a United States person if it is publicly available

3 Foreign intelligence Subject to the special limitations contained in section E , below, information may be collected about a United States person if the in constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are

(a) Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power

(b) An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power,

(c) Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities (See AR 190–52),

(d) Persons who are reasonably believed to be prisoners of war, missing in action, or art the targets, the hostages, or victims of international terrorist organizations, or

(e) Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations or persons

4 Counterintelligence Information may be collected about a United States person if the information constitutes counterintelligence, provided the international collection of counterintelligence about United States persons must be limited to

(a) Person who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities (See AR 190–52, AR 381–12, and AR 381–20)

(b) Persons in contact with persons described in paragraph C 4 a , above, for the purpose of identifying such persons and assessing their relationship with persons described in paragraph C 4 a , above

5 Potential sources of assistant to intelligence activities Information may be collected about United States person reasonably believed to be potential sources of intelligence, or potential sources of assistant to intelligence activities, for the purpose of assessing their suitability and credibility This category does not include investigations undertaken for personnel security purposes (See subsection 8)

6 Protection of intelligence sources and methods Information may be collected about a United States person who has access to, had access to, or is otherwise in possession of, information which reveals foreign intelligence and counterintelligence sources or methods, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information, provided that within the United States, intentional collection of such information shall be limited to persons who are

(a) Present and former DoD employees,

(b) Present or former employees of a present or former DoD contractor, and

(c) Applicants for employment at DoD or at a contractor of DoD

7 Physical security Information may be collected about the United States person who is reasonably believed to threaten the physical security of DoD employees, installations, operations or official visitors Information may also be collected in the course of a lawful physical security investigation (See AR 381–12, AR 381–20, AR 190–1, and AR 190–52)

8 Personnel security Information may be collected on a United States person that arises out of a lawful personnel security investigation This includes information concerning relatives and associates of the subject of the investigation, if required by the scope of the investigation and the information has a bearing on the matter being investigated or the security determination being made (See AR 604–5, AR 381–12, AR 381–20, and AR 190–52)

9 Communications security Information may be collected about a United States person that arises out of a lawful communications security investigation (See AR 380–53)

10 Narcotics Information may be collected about a United States person who is reasonably believed to be engaged in international narcotics activities

11 Threats to safety Information may be collected about a United States person when the information is needed to protect the safety of any person or organization, including those who are targets, victims or hostages of international terrorist organizations (See AR 190–52)

12 Overhead reconnaissance Information may be collected for overhead reconnaissance not directed at specific United States persons

13 Administrative purposes Information may be collected about a United States person that is necessary for administrative purposes

D. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS

1 Means of collection DoD intelligence components are authorized to collect information about United States persons by any lawful means, provided that all such collection activities shall be carried out in accordance with E O 1233, (reference (a)), and this Regulation, as appropriate

2 Least intrusive means The collection of information about United States persons shall be accomplished by the least intrusive means In general, this means–

(a) To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned,

(b) If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources,

(c) If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General, then

(d) If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought

3 Requests to engage in collection techniques which require HQDA or higher level approval will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310 Full justification as required in the relevant procedures will be included

E. SPECIAL LIMITATION ON THE COLLECTION OF FEDERAL INTELLIGENCE WITHIN THE UNITED STATES

Within the United States, foreign intelligence concerning United States persons may be collected only by overt mean unless all the following conditions are met

1 The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any United States person,

2 Such foreign intelligence cannot be reasonable obtained by overt means,

3 The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI), and

4 The use of other than overt means has been approved in writing by the head of the DoD intelligence components concerned, or his single designee, as being consistent with these procedures The Assistant Chief of Staff for Intelligence, HQDA, and the Commanding General, US Army Intelligence and Security Command (INSCOM), are the heads of the Army intelligence components for this purpose Information copies of approval by the Commanding General, INSCOM, will be provided to HQDA(DAMI–CIC), WASH DC 20310, they will reflect appropriate coordination with the supporting judge advocate A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy) All submissions to the Deputy Under Secretary of Defense (Policy) will be forwarded to HQDA(DAMI–CIC), WASH DC 20310

Part 3
PROCEDURES 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

A APPLICABILITY

This procedures governs the kinds of information about United States person that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns It does not apply when the information in question is retained solely for administrative purpose or is required by law to be maintained

B EXPLANATION OF UNDEFINED TERMS

The terms "retention," as used in this procedure, refers only to the maintenance of information about United States persons which can be retrieved by reference to the person's name or other identifying data

C CRITERIA FOR RETENTION

1 Retention of information collected under Procedure 2 Information about United States persons may be retained if it was collected pursuant to Procedure 2

2 Retention of information acquired incidentally Information about United States persons collected incidentally to authorize collection may be retained if

(a) Such information could have been collected intentionally under Procedure 2,

(b) Such information is necessary to understand or access foreign intelligence or counterintelligence,

(c) The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation, or

(d) Such information is incidental to authorized collection and may indicate involvement in activities that may violate federal, state, local, or foreign law

3 Retention of information relating to functions of other DoD Components or non–Dod Agencies Information about United States persons that pertains solely to the functions of other DoD Components or agencies outside the Department of Defense shall be retained only as necessary to transmit or deliver scheduled information to the appropriate recipients

4 Temporary retention Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures

5 Retention of other information Information about United States persons other than that covered by subsection C 1 through 4, above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary

D ACCESS AND RETENTION

1 Controls on access to retained information Access within a DoD intelligence component to information about United States persons retained pursuant to this procedure shall be limited to those with a need to know

2 Duration of retention Disposition of information about United States persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained Information about US persons retained in the files of DA intelligence components will be reviewed This review will insure the following that its continued retention serves the purpose for which it was collected and stored, and that it is necessary to the conduct of authorized functions of DA intelligence components or other Government agencies This review will be conducted in conjunction with the annual review of files under AR 340–2 or AR 340–18–1, as appropriate Review of files in the Intelligence Records Repository (IRR) will be under AR 381–45 and AR 340–18–5 Final disposition of such information will comply with disposition schedules approved by the Archivist of the United States for the files or records in which the information is stored (An example is the AR 340–18 series)

3 Information acquired prior to effective date Information acquired prior to the effective date of this procedure may be retained by DoD intelligence components without being screened for compliance with this procedure or Executive Order 12333 (reference (a)), so long as retention was in compliance with applicable law and previous executive orders

E CONTROL OF ELECTRONIC SURVEILLANCE INFORMATION

1 Review All electronic surveillance information acquired through Army intelligence operations or received from cooperating (liaison) sources will be review expeditiously after receipt This review will assure that the contents are relevant to the purpose of the electronic surveillance coverage All irrelevant or unnecessary information will be destroyed Information about US persons may be collected, retained, or disseminated only if authorized under procedures 2, 3, or 4

2 Access controls Access to electronic surveillance information will be controlled by the commander of the element that is the custodian of the information Procedures will be established to assure that access to electronic surveillance information is limited to those with a need–to–know

3 Annotation Each message, document, report, or file of any type that contains electronic surveillance information which identifies any person or organization by name will be clearly and conspicuously marked with the following annotation "Contents include

electronic surveillance information Handle in accordance with AR 381–10"

F. INDEXING ELECTRONIC SURVEILLANCE INFORMATION

1 General In order to be responsive to motions for discovery under section 3504 title 18, United States Code (18 USC 3504), indices will be maintained of all electronic surveillance information which is used, retained, or disseminated by Army intelligence components and which contain references to an identifiable US or non–US person A person is identifiable if sufficient information is available to the component to determine the last name of the person and to distinguish that person from others who may have the same name A person generally will be considered distinguishable that person from others with the same name when the information required by one or more of subsections 3b–e and g is known Electronic surveillance information that is destroyed without being used, retained, or disseminated need not be indexed

2 Indexing office Headquarters, INSCOM, will maintain an index of all electronic surveillance information obtained by Army intelligence elements worldwide, under provisions of this regulation

3 Content The indices will contain the following information to the extent known

(a) Name and sex of each identifiable person whose communications were intercepted

(b) Language in which the conversation occurred

(c) Telephone numbers, radio frequencies, or radio telephone call signs involved in the interception

(d) Address of the premises at which the surveillance was conducted

(e) Title or number of investigative file

(f) Element maintaining the case file

(g) Date or dates of the interception

4 Retrieval Information maintained in the indices must be retrievable by the following

(a) Name of the subject of the case

(b) Name of each identifiable person overheard, provided that person's conversation was used, retained, or disseminated Retrieval through additional criteria may be imposed on a case–by–case basis by the approving authority

5 Notifying the indexer Promptly after screening of electronic surveillance information (secretary F 1) an electrical message containing the information required by section F 3 will be sent to HQ INSCOM, Fort Meade, MD//IACSF–IRC//, subject Electronic Surveillance Indexing Material

6 Procedure for forwarding backup material Copies of all indexed electronic surveillance information must be sent to HQ INSCOM to serve as backup for the index When this information is contained in an investigative file, it will be sent after the file is closed or the investigation is completed Information not part of an investigative file will be sent as soon as practicable Backup material sent to the indexing office will include the following

(a) Be clearly marked as electronic surveillance information

(b) Refer to the message or messages that transmitted the indexing information

(c) Contain all the electronic surveillance information that was used retained or disseminated

(d) Contain a record of all dissemination's of the information outside the DoD

(e) Carry a certification by the forwarding office)to include name, grade and title) that the contents need the retention criteria of this regulation If the contents include US person information

7 Index security controls Indexing offices will devise procedures to safeguard and control access to the indices and backup material

Part 4
PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

A APPLICABILITY AND SCOPE

This procedures governs the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information It does not apply to information collected solely for administrative purposes, or disseminated pursuant to law, or pursuant to a court order that otherwise imposes controls upon such dissemination

B CRITERIA FOR DISSEMINATION

Except as provided in section C , below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions

1 The information was collected or retained or both under Procedures 2 and 3,

2 The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following

(a) An employee of the Department of Defense, or an employee of a contractor of the Department of Defense, and has a need for such information in the course of his or her official duties,

(b) A law enforcement entity of federal, state, or local government, and the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce,

(c) An agency within the intelligence community, provided that within the intelligence community, information other than information derived from signals intelligence, may be disseminated to each appropriate agency for the purpose of allowing the recipient agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component,

(d) An agency of the federal government authorized to receive such information in their performance of a lawful governmental function, or

(e) A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government

C OTHER DISSEMINATION

Any dissemination that does not conform to the conditions set forth in section B , above, must be approved by the legal office responsible for advising the DoD Component concerned after consultation with the Department of Justice and General Counsel of the Department of Department Such approval shall be based on a determination that the proposed dissemination complies whit applicable laws, executive orders, and regulations Requests will be forwarded through command channels to HQDA (DAMI–CIC), WASH DC 20310

Part 5
PROCEDURE 5 ELECTRONIC SURVEILLANCE

Part 1
ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES

A APPLICABILITY

This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1978 (50 USC 1801, et seq , reference b) and applies to electronic surveillance, as defined in the Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act This part applies to all nonconsensual electronic surveillance conducted within the United States, whether directed against a US or non–US

person Policy and procedures governing all consensual electronic surveillance are found at section C of this part

B. GENERAL RULES

1 Electronic surveillance pursuant to the Foreign Intelligence Surveillance Act A DoD intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes only pursuant to an order issued by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978 (reference (b)), or pursuant to a certification of the Attorney General issued under the authority of section 102(a) of the Act

2 Authority to request electronic surveillance Authority to approve the submission of applications or requests for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (reference (b)) shall be limited to the Secretary of Defense, the Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency Applications for court orders will be made through the Attorney General after prior clearance by the General Counsel, DoD Requests for Attorney General certification shall be made only after prior clearance by the General Counsel, DoD

(a) Requests by Army intelligence components for authority to conduct electronic surveillance pursuant to this part will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310 Requests will include the information required by section C of part 2 of procedure 5, they will be submitted as soon in the planning stage as possible

(b) Policy governing control and indexing of electronic surveillance information is contained in sections E and F, procedure 3

3 Electronic surveillance in emergency situations

(a) A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General in accordance with section 105(e) of reference (b)

(b) The head of any DoD intelligence component may request that the DoD General Counsel seek such authority directly from the Attorney General in an emergency, if it is not feasible to submit such request through an official designated in subsection B 2 . above, provided the appropriate official concerned shall be advised of such requests as soon as possible thereafter

(c) Requests by Army intelligence components for emergency authority to conduct electronic surveillance pursuant to this part will be submitted through command channels to HQDA (DAMI–CIC) WASH DC 20310

C CONSENSUAL ELECTRONIC SURVEILLANCE

1 Applicability This section governs consensual electronic surveillance conducted by Army intelligence components, under the following whether directed against US or non–US persons, and whether occurring within or outside the United States

2 Explanation of undefined terms Consensual electronic surveillance occurs when electronic surveillance is conducted after consent for the interception is given by one or more, but fewer than all, of the parties to the communication

3 Case approval authority

(a) Consensual electronic surveillance conducted within the United States or directed against US persons will be approved in advance by the Secretary or Under Secretary of the Army, or the Army General Counsel Requests for approval will be forwarded through command channels HQDA (DAMI–CIC), WASH DC 20310, they will contain the information required in section C 4 b

(b) Consensual electronic surveillance directed against non–US persons aboard may be approved by those officials identified in procedure 5, part 2, section F 1 This authority may be delegated, in writing, to field supervisors

4 Case approval standards

(a) Consensual electronic surveillance may be conducted for any lawful function assigned the Army intelligence component

(b) Requests for consensual electronic surveillance conducted within the United States or directed against a US person abroad will provide the following

(1) Description of the facts and circumstances requiring the intended interception, the means by which it would be conducted, the place at which it would be conducted, and its expected duration

(2) Names of all persons whose conversations are expected to be intercepted, and their roles in the incident being investigated Except in extraordinary situations, written consent forms will be executed by all individuals consenting to the electronic surveillance In extraordinary situations, the request for surveillance will contain an explanation of why written consent could not be obtained

(3) Statement that in the judgment of the person making the request, the interception is warranted in the interest of a lawful function assigned the Army intelligence component The function will be identified

(c) All electronic surveillance information used, retained, or disseminated, that pertains to an identifiable US or non–US person, must be controlled and indexed pursuant to procedure 3, sections E and F

5 Consensual electronic surveillance in emergency situations Notwithstanding section C 3 a , an Army intelligence component may conduct consensual electronic surveillance within the United States or directed against a US person outside the United States in emergency situations, under the following limitations

(a) A general court–martial convening authority may authorize consensual electronic surveillance He may do so only when securing the prior approval of person described in section C 3 a is not practical because of the reasons listed below

(1) Time required would cause failure or delay in obtaining valuable intelligence information, or

(2) A person's life or physical safety is reasonably believed to be in immediate danger, or

(3) Physical security of a defense installation or Government property is reasonable believed to be in immediate danger

(b) Such officials will notify HQDA (DAMI–CIC), WASH DC 20310, within 24 hours of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results

(c) Concensual electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the persons designated in section C 3 a

Part 2
ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

A APPLICABILITY

This part of Procedure 5 applies to electronic surveillance, as defined in Appendix A, for foreign intelligence and counterintelligence purposes directed against United States person who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy (Electronic surveillance directed against a US person abroad also may be performed pursuant to this part of procedure 5 for any other lawful function assigned an Army intelligence component) It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part I and the regulation of "signals intelligence activities" under Part 3, so that the intentional interception for foreign intelligence and counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts In addition, this part governs the use of electronic, mechanical, or other surveillance devices for foreign intelligence and counterintelligence purposes against a United States person abroad in circumstances where such person has a reasonable expectation of privacy This part does not apply to the electronic surveillance of communications of other than United States person abroad or to the interception of the communications of United States persons abroad that do not constitute electronic surveillance (Policy governing electronic surveillance of non–US persons conducted outside the United States is contained in

sections F and G, below Policy governing control and indexing of electronic surveillance information is contained in procedure 3, sections E and F Policy governing all consensual electronic surveillance is found at procedure 5, section C, part 1

B. EXPLANATION OF UNDEFINED TERMS

1 Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person Electronic surveillance directed against person who are not United States persons that results in the incidental acquisition of the communications of a United States person does not thereby become electronic surveillance directed against a United States person However, use, retention or dissemination of inadvertently intercepted US person communications is governed by section G 4

2 Electronic surveillance is "outside the United States" if the person against whom the electronic surveillance is directed is physically outside the United States, regardless of the location at which surveillance is conducted For example, the interception of communications that originate and terminate outside the United States can be conducted from within the United States and still fall under this part rather than Part 1

C PROCEDURES

Except as provided in section D , below, DoD intelligence components may conduct electronic surveillance against a United States person who is outside the United States for foreign intelligence and counterintelligence purposes only if the surveillance is approved by the Attorney General Request for approval will be forwarded to the Attorney General by an official designated in section E 1 , below Each request shall include

1 An identification or description of the target If applicable, include the address, telephone number, room number, whether inside or outside a building, and whether on public or private property

2 A statement of the facts supporting a finding that

(a) There is probable cause to believe the target of the electronic surveillance is one of the following

(1) A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities,

(2) A person who is an officer or employee of a foreign power,

(3) A person unlawfully acting for, or pursuant to the direction of, a foreign power The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power,

(4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power, or

(5) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access

(b) The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence

(c) The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be contained by other less intrusive collection techniques

3 A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance

4 A description of the means by which the electronic surveillance will be effected Describe the equipment to be used, method of transmission, recording device, and method of installation

5 If physical trespass is required to effect the surveillance, a statement of facts supporting a finding that the means involve the least amount of intrusion that will accomplish the objective

6 A statement of period of time, not to exceed 90 days, for which the eligibility surveillance is required

7 A description of the expected dissemination of the product of the surveillance, including a description of the procedures that will govern the retention and dissemination of communications or concerning United States persons other that those targeted, acquired incidental to such surveillance

8 A description of any less intrusive procedures that have been tried and failed, why they may fail again, or why they are too dangerous to attempt

9 If the request is for an extension of a previous authorization, describe results thus far obtained from the interception, or give a reasonable explanation of the failure to obtain results

10 Indicate that the request has been coordinated with the appropriate staff or command judge advocate

11 If known, indicate whether previous requests have been made for electronic surveillance on any of the same persons, facilities, or places to be surveyed State whether such requests were approved or disapproved

D ELECTRONIC SURVEILLANCE IN EMERGENCY SITUATION

Notwithstanding section C , above, a DoD intelligence component may conduct surveillance directed at a United States person who is outside the United States in emergency situations under the following limitations

1 Officials designated in section E , below, may authorize electronic surveillance directed at a United States person outside the United States in emergency situations, when securing the prior approval of the Attorney General is not practical because

(a) The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security,

(b) A person's life or physical safety is reasonably believed to be in immediate danger, or

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger

2 Except for actions taken under subsection D 1 b , above, any official authorizing such emergency surveillance shall find that one of the criteria contained in subsection C 2 a , above, is met Such officials shall notify the DoD General Counsel promptly of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results

3 The Attorney General shall be notified by the General Counsel, DoD, as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and such other information as may be required to authorize continuation of such surveillance

4 Electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours

E OFFICIALS AUTHORIZED TO REQUEST AND APPROVE ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES

1 The following officials may request approval of electronic surveillance of US persons outside the United States under section C , above, and approved emergency surveillance under section D , above,

(a) The Secretary and Deputy Secretary of Defense

(b) The Secretaries and Under Secretaries of the Military Departments

(c) The Directory and Deputy Directory of the National Security Agency/Chief, Central Security Service

2 Authorization for emergency electronic surveillance under section D, may also be granted by

(a) Any general or flag officer at the overseas location in question, having responsibility for either the subject of them surveillance, or responsibility for the protection of persons, installations, or property that is endangered (Before an Army general officer is an overseas location authorizes and emergency electronic surveillance, he or she must coordinate with the major Army command (MACOM) senior intelligence officer (SIO) and supporting judge advocate on appropriateness and applicable policy regarding the proposed surveillance When an Army general officer at an overseas location authorizes an emergency electronic surveillance, the MACOM SIO will provide details to HQDA (DAMI–CIC), WASH DC 20310, by the most expeditious means available), or

(b) The Deputy Director for Operations, National Security Agency

F ELECTRONIC SURVEILLANCE OF NON–US PERSONS

This section prescribes the sole authority by which Army intelligence components may engage in non–consensual electronic surveillance of non–US persons outside the United States Electronic surveillance of non–US persons within the United States is governed by part 1 of procedure 5 Consensual electronic surveillance is governed by section C of part 1 of procedure 5

1 Case approval authority Authorities listed below may approve electronic surveillance under this section that is conducted by Army intelligence components or requested directly or indirectly by those components

(a) The Assistant Chief of Staff for Intelligence (ACSI), HQDA

(b) Commanding General, INSCOM

(c) Commander in Chief, US Army, Europe, and Seventh Army (CINCUSAREUR)

(d) *Commanding General Eighth United States Army (EUSA)* The officials at (a) through (d) above may delegate authority to their deputies, chiefs of staff, or ranking intelligence staff officers, they in turn may delegate their authority to the responsible military intelligence group commanders No further delegation is authorized All delegation of authority will be in writing Requests for approval will be forwarded through command channels, they will contain the information required in section 2 (a) through (I) Approval will be granted only after coordination will the approving authority's sup porting judge advocate Information copies of approvals will be provided to HQDA (DAMI–CIC), WASH DC 20310

2 Case approval standards Non–consensual electronic surveillance of non–US persons abroad may be conducted for any lawful functions assigned the Army intelligence component Each reques' to conduct electronic surveillance pursuant to this section will com ply with the following

(a) Provide facts sufficient to support a determination by the approval authority that a reasonable belief exists that the surveil lance will gather valuable intelligence information

(b) Describe nature and content of conversations expected to be intercepted

(c) Identify the investigative unit that will conduct the surveillance

(d) Identify any US persons whose communications could reasonably be expected to be intercepted Identify any people who have consented to the surveillance

(e) Describe the equipment to be used and the method of installation

(f) State the location of the proposed surveillance If applicable include the address and means of access If physical trespass is required, detail the method of entry

(g) Estimate the expected duration of the surveillance

(h) If the request is for an extension of a previous authorization, describe the results thus far obtained, or provide an explanation of the failure to obtain results

(i) Indicate that the request has been coordinated with the appropriate judge advocate and the date of the coordination

3 Case approval periods Initial approvals of cases directed against non–US persons may be granted for a period up to 90 days Renewal requests for non–US person cases involving specific individuals may be approved for a period up to 90 days Renewal requests for cases involving foreign intelligence or counterintelligence of a continuing and long–term interest may be approved for a period up to 1 year All renewal requests will be submitted in the same manner as the original request, they will be reviewed under the same criteria

4 Inadvertent interception of US person conversations If a US person communication is inadvertently intercepted during electronic surveillance directed against a non–US person, the following will apply

(a) Approval of the Secretary or Under Secretary of the Army must be obtained before the information is used, retained or disseminated Requests for approval should be sent through command channels to HQDA (DAMI–CIC), WASH DC 20310

(b) In emergency situations such request may be approved by the Army General Officer, after coordination with his or her senior intelligence officer A report of emergency approvals will be expeditiously provided to HQDA (DAMI–CIC), WASH DC 20310 The report will include an explanation of the nature of the emergency situation

(c) Electronic surveillance information approved for use, retention, or dissemination under this subsection must be controlled and indexed pursuant to sections E and F, procedure 3

(d) Approval of the Secretary and Under Secretary of the Army is not required if the contents of the inadvertent interception are destroyed and are not used, retained, or disseminated

Part 3
SIGNALS INTELLIGENCE ACTIVITIES

A APPLICABILITY AND SCOPE

1 This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involves the collection, retention, and dissemination of foreign communications and military tactical communications Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto

2 This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/ Chief, Central Security Service, which shall also be approved by the Attorney General That regulation shall provide that signals intelligence activities which constitute electronic surveillance as defined in Parts 1 and 2 of this procedure, will be authorized in accordance with those parts Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the Attorney General

B EXPLANATION OF UNDEFINED TERMS

1 Communications concerning a United States person are those in which the United States person is identified in the communication A United States person is identified when the person's name, unique title, address or other personal identifier is revealed in the communication in the context of activities conducted by that person A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Monroe Doctrine," is not an identification of a United States person

2 Interception means the acquisition by the United States Signals Intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signals

3 Military tactical communications means United States and allied military exercise communications within the United States and

abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communication security

4 United States person For purpose of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person

(a) A person known to be currently in the United States will be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is not a United States citizen or permanent resident alien

(b) A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien

(c) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien

(d) An unincorporated association whose headquarters are located outside the United States may be presumed not the be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence

5 United States Signals Intelligence System means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the military services authorized to conduct signals intelligence and such other entities (other than the Federal Bureau of Investigation) as are authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence FBI activities are governed by procedures promulgated by the Attorney General

C. PROCEDURES

1 Foreign communications The United States Signals Intelligence System may collect, process. retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure

2 Military tactical communications The United States Signals Intelligence System may collect, process, retain. and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure

(a) *Collection* Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercise

(b) *Retention and processing* Military tactical communications may be retained and processed without deletion of references to United States persons who are participants in, or are otherwise mentioned in exercise–related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible

(c) *Dissemination* Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating in or conducting review and critiques of such exercise

Part 4
TECHNICAL SURVEILLANCE COUNTERMEASURES

A APPLICABILITY AND SCOPE

This part of Procedure 5 applies to the use of electronic equipment to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance It implements section 105(f)(2) of the Foreign Intelligence Surveillance Act, (reference b))

B. EXPLANATION OF UNDEFINED TERMS

The term technical surveillance countermeasures refers to activities authorized pursuant to DoD Directive 5200.29, (reference (c)), and, as used in the procedure, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, or for determining the susceptibility of electronic equipment to unlawful electronic surveillance

C. PROCEDURES

A DoD intelligence component may use technical surveillance countermeasures that involve the incidental acquisition of the nonpublic communications of United States persons without their consent, provided

1 The use of such countermeasures has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken,

2 The use of such countermeasures is limited in extent and duration to that necessary to determine the existence and capability of such equipment, and

3 Access to the content of communications acquired during the use of countermeasures is limited to person involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use However, if the content is acquired within the United States, only information which is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (d)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated to appropriate law enforcement authorities A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained

4 Use, retention, or dissemination of US person information acquired pursuant to this part must be approved by the Secretary or Under Secretary of the Army Requests should be submitted to HQDA dm, WASH DC 20310 In emergency situations such request may be approved by any Army general officer, after consultation with his or her senior intelligence officer and supporting judge advocate A report will contain an explanation of the nature of the emergency situation

Part 5
DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENT

A APPLICABILITY

This part of Procedure 5 applies to developing, testing, and calibrating electronic equipment that can intercept or process communications and non–communications signals It also includes research and development that needs electronic communications as a signal source

B PROCEDURES

1 Signal Authorized for Use

(a) The following may be used without restrictions

(1) Laboratory–generated signals

(2) Communications signals with the consent of the communicator

(3) Communications in the commercial or public service broadcast bands

(4) Communications transmitted between terminals located outside of the United States not used by any known United States person

(b) Communications subject to lawful electronic surveillance under the provisions of Parts 1, 2, or 3 of this procedure may be used subject to the minimization procedures applicable to such surveillance

(c) Any of the following may be used subject to the restrictions of subsection B 2 , below

(1) Communications over official government communications circuits with consent from an appropriate official of the controlling agency

(2) Communications in citizens and amateur–radio bands

(d) Other signals may be used only where it is determined that it is not practical to use the signals described above and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance The restrictions of subsection B 2 , below will apply in such cases The Attorney General must approve use of signals pursuant to this subsection for the purpose of development, testing, or calibration when the period of use exceeds 90 days When Attorney General approval is required, the DoD intelligence component shall submit a test proposal to the General Counsel, DoD, or the NSA General Counsel for transmission to the Attorney General for approval The test proposal shall state the requirement for a period beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity Requests will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310

2 Restrictions For signals described in subsection B 1 c and d , above, the following restrictions apply

(a) The surveillance shall be limited in scope and duration to that necessary for the purpose referred to in section A above

(b) No particular United States person shall be targeted intentionally without consent

(c) The content of any communication shall

(1) Be retained only when actually needed for the purposes referred to in section A above

(2) Be disseminated only to persons conducting the activity, and

(3) Be destroyed immediately upon completion of the activity

(d) The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes outlined in section A , above, or for collection avoidance purposes Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment provided such dissemination and use are limited to the purposes outlined in section A , or collection avoidance purposes No content of any communication may be retained or used other than as provided in subsection B 2 c , above

Part 6
TRAINING OF PERSONNEL IN THE OPERATIONS AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

A APPLICABILITY

This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operations and use of electronic communications and surveillance equipment It does not apply to the interception of communications with the consent of one of the parties to the communication or to the training of intelligence personnel by nonintelligence components

B. PROCEDURES

1 Training guidance The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment shall include guidance concerning the requirements and restrictions of the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and E O 12333 (reference (a)), with respect to the unauthorized acquisition and use of the content of communications of United States persons

2 Training Limitations

(a) Except as permitted by subsection B 2 b and c , below, the use of electronic communications and surveillance equipment for training purposes is permitted subject to the following limitations

(1) To the maximum extent practical, use of such equipment for training purposes shall be directed against communications which are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure

(2) The contents of private communication of nonconsenting United States persons may not be acquired aurally unless the person is an authorized target of electronic surveillance

(3) The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment

(b) Public broadcasts, distress signals, or official United States Government communications may be monitored, provided that when government agency communications are monitored, the consent of an appropriate official is obtained

(c) Minimal acquisition of information is permitted as required for calibration purposes

3 Retention and dissemination Information collected during training that involves communications described in subsection B 2 a (1), above, shall be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance Information collected during training that does not involve communications described in subsection B 2 a (1), above, or that is acquired inadvertently, shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose This subsection does not apply to distress signals

Part 7
CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS

A APPLICABILITY AND SCOPE

This part of Procedure 5 applies to the conduct of vulnerability surveys and hearability surveys by DoD intelligence components Army implementation is contained in AR 380–53

B EXPLANATION OF UNDEFINED TERMS

1 The term vulnerability survey refers to the acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by g intelligence services

2 The term hearability survey refers to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the quality of reception over time

C PROCEDURES

1 Conduct of vulnerability surveys Nonconsensual surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of transmission facilities of communications common carriers, other private commercial entities, and entities of the federal government, subject to the following limitations

(a) No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee

(b) No transmission may be acquired aurally

(c) No content of any transmission may be acquired by any means

(d) No transmission may be recorded

(e) No report or log may identify any United States person or

entity to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be disseminated Logs may be disseminated only if required to verify results contained in reports

2 Conduct of hearability surveys The Director, National Security Agency may conduct, or may authorize the conduct by other agencies, of hearability surveys of telecommunications that are transmitted in the United States

(a) *Collection* Where practicable, consent will be secured from the owner or user of the facility against which the hearability survey is to be conducted prior to the commencement of the survey

(b) *Processing and Storage* Information collection during a hearability survey must be processed and stored as follows

(1) The content of communications may not be recorded or included in any report

(2) No microwave transmission my be demultiplexed or demodulated for any purpose

(3) No report or log may identify any person or entity except to the extent of identifying the transmission facility that can be intercepted from the intercept site If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the hearability survey has been conducted, the identity of such users may be obtained provided such identities may not be obtained from the contents of the transmission themselves

(a) *Dissemination* Reports may be disseminated only within the United States Government Logs may not be disseminated unless required to verify results contained in reports

Part 6
PROCEDURE 6 CONCEALED MONITORING

A APPLICABILITY AND SCOPE

1 This procedure applies to concealed monitoring only for foreign intelligence and counterintelligence purposes conducted by a DoD intelligence component within the United States or directed against a United States person who is outside the United States where the subject of such monitoring does not have a reasonable expectation of privacy as explained in section B , below, and no warrant would be required if undertaken for law enforcement purposes

2 Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes where the subject of such monitoring (whether or not a US person) has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure

3 Concealed monitoring for foreign intelligence and counterintelligence purposes of a United States person abroad where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as 'electronic surveillance outside the United States" under Part 2 of Procedure 5, and processed pursuant to that procedure

4 Concealed monitoring for foreign intelligence and counterintelligence purposes when the monitoring is a signals intelligence activity shall be conducted pursuant to Part 3 of Procedure 5

5 Concealed monitoring for foreign intelligence and CI purposes of a non–US persona broad who has a reasonable exceptional of privacy will be treated as electronic surveillance of a non–US person outside the United States This is governed by section F of part 2 of procedure 5

B EXPLANATION OF UNDEFINED TERMS

1 Concealed monitoring means targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it Monitoring is continuous if it is conducted without interruption for a substantial period of time Beacons ("beepers") and transponders generally are considered methods of concealed monitoring under the following conditions when affixed in a public place (for example, placing the device on the underside of a vehicle on a public area), and where no warrant would be required in a criminal law context Concealed monitoring by "beacons" authorized under this procedure must terminate when the target of the monitoring acquires an expectation of privacy An example would be the vehicle entering private property not visible from a public place

2 Monitoring is within the United States if the monitoring device, or the target of the monitoring, is located within the United States

3 Whether concealed monitoring is to occur where the subject has a reasonable exception of privacy is a determination which depends upon the circumstances of a particular case, and shall be made only after consultation with the legal off responsible for advising the DoD intelligence component concerned Reasonable expectation of privacy is the extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to monitoring by electronic, optical, or mechanical devices For example, there are ordinarily reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal working conditions Conversely, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed, however, such a person ordinarily would have an expectation of privacy within his or her residence

C PROCEDURES

1 Limitations on use of concealed monitoring Use of concealed monitoring under circumstances when the subject of such monitoring has no reasonable expectation of privacy is subject to the following limitations

(a) Within the United States, a DoD intelligence component may conduct concealed monitoring only on an installation and facility owned or leased by DoD, or otherwise in the course of an investigation conducted pursuant to the Agreement Between the Secretary of Defense and the Attorney General, reference (g) (See App B)

(b) Outside the United States, such monitoring may be conducted on installation and facilities owned or leased by the Department of Defense Monitoring outside such facilities shall be conducted after coordination with appropriate host country officials, if such coordination is required by the governing Status of Forces Agreement, and with the Central Intelligence Agency

2 Required Determination Concealed monitoring conducted under subsection C 1 , requires approval by an official designated in subsection C 3 , below, based on a determination that such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions, and does not constitute electronic surveillance under Parts 1 or 2 of Procedure 5

3 Officials authorized to approve concealed monitoring Officials authorized to approve concealed monitoring under this procedure include the Deputy Under Secretary of Defense (Policy), the Director, Defense Intelligence Agency, the Director, National Security Agency, the Assistant Chief of Staff for Intelligence, Department of Army, the Director, Naval Intelligence, the Director of Intelligence, U S Marine Corps, the Assistant Chief of Staff, Intelligence, United States Air Force, the Commanding General, Army Intelligence and Security Command, the Director, Naval Investigative Service, and the Commanding Officer, Air Force Office of Special Investigations

(a) Requests for approval of concealed monitoring will be coordinated with the legal advisor to the approving authority

(b) Information copies of approvals by the Commanding General, INSCOM, will be provided to HQDA (DAMI–CIC), WASH DC 20310

Part 7
PROCEDURE 7 PHYSICAL SEARCHES

A. APPLICABILITY

This procedure applies to unconsented physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes Physical searches also may be performed pursuant to this procedure for any other lawful function assigned an Army intelligence component DoD intelligence components may provide assistant to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12 Part C 4 of this procedure also governs physical searches on non–US persons abroad

B EXPLANATION OF UNDEFINED TERMS

Physical search means any intrusion upon a person or a person's property of possessions to obtain items of property or information The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place The term also does not include any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to Parts 1 and 2 of Procedure 5

C PROCEDURES

1 Unconsented physical searches within the United States

(a) *Searches of active duty military personnel for counterintelligence purposes* The counterintelligence elements of the Military Departments are authorized to conduct unconsented physical searches in the United States for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military judge, or a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers For purposes of this section, the term 'agent of a foreign power" refers to an individual who meets the critical set forth in subsection C 2 b (2), below

(b) *Other unconsented physical searches* Except as permitted by section A , above, DoD intelligence components may not conduct unconsented physical searches of person and property within the United States for foreign intelligence or counterintelligence purposes DoD intelligence components may, however, request the FBI to conduct such searches All such requests shall be in writing, shall contain the information required in section C 2 b (1) through (6), below, and be approved by an official designated in section C 2 c , below A copy of each such request shall be furnished the General Counsel, DoD

2 Unconsented physical searches outside the United States

(a) *Searches of active duty military personnel for counterintelligence purposes* The counterintelligence elements of the Military Departments may conduct unconsented physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes when authorized by a military judge, or a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198, (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the critical set forth in subsection C 2 b (2), below

(b) *Other unconsented physical searches* DoD intelligence components may conduct other unconsented physical searches for foreign intelligence and counterintelligence purposes of the person or property of United States persons outside the United States only pursuant to the approval of the Attorney General Requests for such approval will be forwarded by a senior official designated in subsection C 2 c , below, to the Attorney General and shall include

(1) An identification of the person or description of the property to be searched

(2) A statement of facts supporting a finding that there is probable cause to believe the subject of the search is

(a) A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities

(b) A person who is an officer or employee of a foreign power,

(c) A person unlawfully acting for, or pursuant to the direction of, a foreign power The mere fact that a person's activities may benefit or further the aims of a foreign power does not justify an unconsented physical search without evidence that the person is taking direction from, or acting in knowing concert site, the foreign power,

(d) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power, or

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access

(3) A statement of facts supports a finding that the search is necessary to obtain significant foreign intelligence or counterintelligence

(4) A statement of facts supporting a finding that the significant foreign intelligence or counterintelligence expected to be obtained could not be obtained by less intrusive means

(5) A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search

(6) A description of the extent of the search and a statement of facts supporting a finding that the search will involve the least amount of physical intrusion that will accomplish the objective sought

(7) A description of the expected dissemination of the product of the search, including a description of the procedures that will govern the retention and dissemination of information about United States persons acquired incidental to the search

(c) Request for approval of unconsented physical searches under subsection C 2 b must be made by

(1) The Secretary or the Deputy Secretary of Defense,

(2) The Secretary or the Under Secretary of a Military Department,

(3) The Director, National Security Agency,

(4) The Director, Defense Intelligence Agency

3 Requests for authority to conduct unconsented physical searches within the United States or of US persons abroad

(a) Information copies of approvals for physical searches authorized pursuant to sections C 1 a or C 2 a will be provided to HQDA (DAMI–CIC), WASH DC 20310

(b) Requests submitted by an Army intelligence component under sections C 1 b or C 2 b will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310

4 Uunconsented physical searches of non–US persons abroad

(a) Unconsented physical searches of non–US persons outside the United States may be performed for any lawful function assigned the Army intelligence component

(b) Unconsented physical searches of non–US persons outside the United States may be approved by the following officials

(1) ACSI, HQDA

(2) Commanding General, INSCOM

(3) CINCUSAREUR

(4) Commanding General, EUSA The officials at (1) through (4) above may delegate authority to their deputies, chiefs of staff, or ranking intelligence staff officers, they in turn may delegate their authority to the responsible military intelligence group commanders, who may further delegate this authority to military intelligence battalion commanders or their equivalent No further delegation is

authorized All delegations must be in writing Request for approval will be forwarded through command channels, approvals will be granted only after coordination with the approving authority's supporting judge advocate Information copies of all approvals will be provided to HQDA (DAMI-CIC), WASH DC 20310

Part 8
PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

A. APPLICABILITY

This procedure applies to the opening of mail in United States postal channels, and the use of mail covers with respect to such mail, for foreign intelligence and counterintelligence purposes (Additionally, mail opening and mail covers may be performed pursuant to this procedure for any other lawful function assigned an Army intelligence component) It also applies to the opening of mail to or from United States persons where such activity is conducted outside the United States and such mail is not in United States postal channels

B EXPLANATION OF UNDEFINED TERMS

1 Mail within the United States postal channels includes

(a) Mail while in transit within, among, and between the United States, its territories and possessions (including mail of foreign origin which is passed by a foreign postal administration to the United States Postal Service is forwarding to a foreign post administration under a postal treaty or convention, and mail temporarily in the hands of the United States Customs Service or the Department of Agriculture), Army-Air Force (APO) and Navy (FPO) post offices, and mail for delivery to the United Nations, N Y , and

(b) International mail en route to an addressee in the United States or its possessions after passage to United States Postal Service from a foreign postal administration or en route to an addressee aboard before passage to a foreign postal administration

(c) As a rule, mail shall be considered in such postal channels until the moment it is delivered manually in the United States to the specific addressee named on the envelope, or his authorized agent

2 To examine mail means to employ a mail cover with respect to such mail

3 Mail cover means the process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the postal service

C. PROCEDURES

1 Searches of mail within United States postal channels

(a) Applicable postal regulations do not permit DoD intelligence components to detain or open first class mail within United States postal channels for foreign intelligence or counterintelligence purposes, or to request such action by the U S Postal Service Searches of first class mail in US postal channels may be authorized for law enforcement purposes under procedures established in DoD 4525 6-M, chapter 8, volume I

(b) DoD intelligence components may request appropriate U S postal authorities to inspect, or authorized the inspection, of the contents of second, third or fourth class mail in United States postal channels, for such purposes, in accordance with applicable postage regulations Such components may also request appropriate U S postal authorities to detain, or permit the detention of, mail that may become subject to search under this section, in accordance with applicable postal regulations Request for approval under this subsection will be coordinated with the legal advisor to the approving authority Information copies of request submitted to postal authorities by the Commanding General, INSCOM will be provided to HQDA (DAMI-CIC), WASH DC 20310

2 Searches of mail outside United States postal channels

(a) DoD intelligence components are authorized to open mail to or from the United States person that is found outside United States postal channels only pursuant to the approval of the Attorney General, Requests for such approval shall be treated as a request for an unconsented physical search under subsection C 2 b of Procedure 7 Army intelligence components will submit such requests through command channels to HQDA (DAMI-CIC), was

(b) Heads of DoD intelligence components may authorize the opening of mail outside U S postal channels when both the sender and intended recipient are other than United States persons if such searches are otherwise lawful and consistent with any Status of Forces Agreement that may be in effect Searches of mail pursuant to this subsection may be conducted for any lawful function assigned an Army intelligence component Searches of mail outside US postal channels may be approved by the following officials

(1) ACSI, HQDA

(2) Commanding General, INSCOM

(3) CINCUSAREUR

(4) Commanding General, EUSA The officials at (1) through (4) above may delegate authority to their deputies, chiefs of staff, or ranking intelligence staff officers They in turn may delegate their authority to responsible mil intelligence group commanders, these commanders may further delegate this authority to military intelligence battalion commanders, or equivalent No further delegation is authorized Delegation of authority must be in writing Requests for approval will be forwarded through command channels Approvals will be granted only after coordination with the approving authority's supporting judge advocate Information copies of all approvals will be provided to HQDA (DAMI-CIC), WASH DC 20310

3 Mail Covers

(a) DoD intelligence components may request U S postal authorities to examine mail in U S postal channels, for counterintelligence purposes, in accordance with applicable postal regulations Applicable regulations include AR 65-75, the US Postal Service Domestic Mail Manual, and DoD 4525 6-M

(b) DoD intelligence components may also request mail covers with respect to mail to or from a United States person that is outside U S postal channels, or mail covers on non-US persons outside US postal channels in accordance with appropriate law and procedure of the host government, and any Status of Forces Agreement that may be in effect

(c) Requests for mail covers pursuant to this section may be approved by the same authorities and procedures described in section C 2 b

Part 9
PROCEDURE 9. PHYSICAL SURVEILLANCE

A APPLICABILITY

This procedure applies only to the physical surveillance of United States persons by DoD intelligence components for foreign intelligence and counterintelligence purposes Additionally, physical surveillance may be performed pursuant to this procedure for any other lawful function assigned an Army intelligence component This procedure does not apply to physical surveillance conducted as part of a training exercise where the subjects are participants in the exercise This procedure also governs physical surveillance of non-US persons

B EXPLANATION OF UNDEFINING TERMS

The terms physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involved electronic surveillance

C PROCEDURES

1 Critical for physical surveillance in the United States Within the United States, DoD intelligence components may conduct unconsented physical surveillance's for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence components concerned, present or former contractors of such components or their

present or former employees, applicants for such employment or contracting, or military persons employed by a nonintelligence element of a Military Service Any physical surveillance within the United States that occurs outside a DoD installation shall be coordinated with the FBI and other law enforcement agencies as may be appropriate Army intelligence components additionally may conduct physical surveillance of persons in contact with the above subjects, but only to the extent necessary to identify that person Physical surveillance for identification purposes may be approved by a field supervisor

2 Critical for physical surveillance outside the United States Outside the United States, DoD intelligence components may conduct unconsented physical surveillance of United States persons in one of the categories identified in subsection C 1 , above In addition, such components may conduct physical surveillance of other United States persons in the course of a lawful foreign intelligence or counterintelligence investigation, provided (a) such surveillance is consistent with the laws and policy of the host government and does not violate any Status of Forces Agreement that may be in effect, and (b) that physical surveillance of the United States person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot be obtained by other means Army intelligence components additionally may conduct physical surveillance of persons in contact with the above subjects, but only to the extent necessary to identify that person Physical surveillance for identification purposes may be approved by a field supervisor

3 Required approvals for physical surveillance

(a) Persons within DoD investigative jurisdiction Physical surveillance within the United States of US persons or which involve United States persons within DoD investigative jurisdiction overseas may be approved by the head of the DoD intelligence component concerned or by designated senior officials of such components in accordance with this procedure Persons within DoD investigative jurisdiction are defined in "The agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979," at appendix B Requests for physical surveillance pursuant to this section may be approved by the following officials

(1) ACSI, HQDA

(2) Commanding General, INSCOM

(3) CINCUSAREUR

(4) Commanding General EUSA The officials at (1) through (4) above may delegate authority, in writing, to their deputies, chiefs of staff, or ranking intelligence staff officers No further delegation is authorized Requests for approval will be forwarded through command channels, approval will be granted only after coordination with the approving authority's supporting judge advocate Information copies of all approvals will be provided to HQDA (DAMI–CIC), WASH DC 20310

(b) Persons outside DoD investigative jurisdiction Outside the United States, physical surveillance's of United States persons who are not within the investigative jurisdiction of the DoD intelligence component concerned will be forwarded through appropriate channels to the Deputy Under Secretary of Defense (Policy) for approval Requests for approval of physical surveillance pursuant to this section will be forwarded through command channels to HQDA (DAMI–CIC), WASH DC 20310 Such requests shall indicate coordination with the Central Intelligence Agency

4 Physical surveillance of Non–US Persons

(a) Physical surveillance of non–US persons may be conducted for any lawful function assigned the Army intelligence component

(b) Physical surveillance of non–US persons within the United States may be approved by the ACSI, DA, the Commanding General, INSCOM, or their written designees It must be conducted in conformity with jurisdictional limitations imposed by "The Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979" at appendix B

(c) Officials identified in section C 3 a may approve physical surveillance of non–US persons abroad This authority may be delegated down to field supervisors All delegations must be in writing

Part 10
PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

A APPLICABILITY

This procedure applies to participation by employees of DoD intelligence components in any organization within the United States, or any organization outside the United States that constitutes a United States person, when such participation is on behalf of any entity of the intelligence community These procedures do not apply to participation in organizations for solely personal purposes

B. EXPLANATION OF UNDEFINED TERMS

1 Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization or person

2 The term organization includes corporations and other commercial organizations, academic institutions, clubs, professional societies, associations, and any other group whose existence is formalized in some manner or otherwise functions on a continuing basis

3 An organization within the United States means all organizations physically located within the geographical boundaries of the United States whether or not they constitute a United States person Thus, a branch, subsidiary, or office of an organization with the United States, which is physically located outside the United States, is not considered as an organization within the United States

4 Participation refers to an action undertaken within the structure or framework of the organization involved Such actions include serving as a representative or agent of the organization, acquiring membership, attending meetings not open to the public, including social functions for the organization as a whole, carrying out the work or functions of the organization, and contributing funds to the organization other than in payment for goods or services Actions taken outside the organizational framework, however, do not constitute participation Thus, attendance at meeting or social gatherings which involve organization members but are not functions or activities of the organization itself does not constitute participation

5 Participation is on behalf of an agency within the intelligence community when an employee is asked or requested to take action within an organization for the benefit of such agency Such employee may already be a member of the organization or may be asked to join Actions undertaken for the benefit of an intelligence agency include collecting information, identifying potential sources or contracts, or establishing and maintaining cover If a cooperating source furnishes information to an intelligence agency which he or she obtained by participation within an organization but was not given prior to direction or tasking by the intelligence agency to collect such information, then such participation was not on behalf of such agency

6 Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit

C PROCEDURES FOR UNDISCLOSED PARTICIPATION

Except as permitted herein, employees of DoD intelligence components may participation on behalf of such components in organizations within the United States, or in organizations outside the United States that constitute United States persons, only if their affiliation with the intelligence component concerned is disclosed to an appropriate official of the organization in accordance with section D , above Participation without such disclosure is permitted only if it is consistent with the limitations set forth in subsection C 1 , below, and has been approved in accordance with subsection C 2 , below

1 Limitations on undisclosed participation

(a) *Lawful Purpose* No undisclosed participation shall be permitted under this procedure unless it is essential to achieving a lawful

foreign intelligence or counterintelligence purpose within the assigned mission of the collecting DoD intelligence component

(b) *Limitations on use of undisclosed participation for foreign intelligence purposes within the United States* Undisclosed participation may be authorized within the United States for the purpose of collecting foreign intelligence from or about a United States person, nor to collect information necessary to assess us persons as potential sources of assistant to foreign intelligence activities This does not preclude the collection of information about such persons, volunteered by cooperating sources participating in organizations to which such persons belong, however, if otherwise permitted by Procedure 2

(c) *Duration of Participation* Authorization to participate under subsection C 2 a and b shall be limited to the period covered by such participation which shall be no longer than 12 months Participation which lasts longer than 12 months shall be reapproved by the appropriate official on an annual basis in accordance with this procedure

(d) *Participation for the purpose of influencing the activities of the organization or its members* No participation under this procedure shall be authorized for the purpose of influencing the activities of the organization in question, or its members, unless such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power Any DoD intelligence component that desires to undertake participation for such purpose shall forward its request to the Deputy Under Secretary of Defense (Policy) setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity Such participation may be approved by the DUSD(P) with the concurrence of the General Counsel, DoD Request for approval such participation by Army intelligence elements will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310

2 Required approvals

(a) Undisclosed participation that may be approved within a DoD intelligence component Undisclosed participation on behalf of a DoD intelligence component may be authorized within such component under the following circumstances

(1) Participation in meetings open to the public For purposes of this section, a seminar or conference sponsored by a professional organization that is open to persons of a particular profession whether or not they are members of the organization itself or have received a special invitation, shall be considered a meeting open to the public

(2) Participation in organizations that permits other persons acknowledged to the organization to be employees of the United States Government to participate

(3) participation in educational professional organizations for the purpose of enhancing the professional skills, knowledge, or capabilities of employees

(4) Participation in seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar types of meetings, sponsored by organizations in which the employee is a member, has been invited to participate, or when the sponsoring organization does not require disclosure of the participant s employment affiliations, for the purpose of collecting significant foreign intelligence that is generally made available to participants at such meetings, and does not involve the domestic activities of the organization or its members

(5) Request to engage in undisclosed participation pursuant to this subsection may be approved by the ACSI, HQDA, Commanding General, INSCOM, Deputy Chief of Staff, Intelligence (DCSI), USAREUR, the G–2, EUSA, or their written designees All requests will receive prior legal review by the supporting judge advocate Information copies of approvals will be forwarded to HQDA (DAMI–CIC), WASH DC 20310

(b) Participation that may be approved by senior intelligence officials Undisclosed participation may be authorized by either the Deputy Under Secretary of Defense (Policy), the Director, Defense Intelligence Agency, the Assistant Chief of Staff for Intelligence Department of the Army, the Commanding General, U S Army Intelligence and Security Command, the Director of Naval Intelligence, the Director of Intelligence, U S Marine Corps, the Assistant Chief of Staff, Intelligence, United States Air Force, the Director, Naval Investigation Service, the Commanding Officer, Air Force Office of Special Investigations or their single designees, for the following purposes

(1) To collect significant foreign intelligence outside the United States, or from or about other than United States persons within the United States, provided no information involving the domestic activities of the organization or its members may be collected

(2) For counterintelligence purposes, at the written request of the Federal Bureau of Investigation

(3) To collect significant counterintelligence about other than United States persons, or about United States persons who are within the investigative jurisdiction of the Department of Defense, provided any such participation that occurs within the United States shall be coordinated with the Federal Bureau of Investigation

(4) To collect information necessary to identify and assess other than United States persons as potential sources of assistant for foreign intelligence and counterintelligence activities

(5) To collect information necessary to identify United States persons as potential sources of assistant to foreign intelligence and counterintelligence activities

(6) To develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities

(7) Outside the United States, to assess United States persons as potential sources of assistant to foreign intelligence and counterintelligence activities

(8) Requests to engage in undisclosed participation pursuant to this section must be approved by the ACSI, HQDA, or the Commanding General, INSCOM All request will receive prior legal review by the Office of The Judge Advocate General, HQDA, or the Staff Judge Advocate, INSCOM, respectively Information copies of all approvals by the Commanding General, INSCOM, will be provided to HQDA (DAMI–CIC), WASH DC 20310

D DISCLOSURE REQUIREMENT

1 Disclosure of the intelligence affiliation of an employee of a DoD intelligence component shall be made to an executive officer of the organization in question, or to an official in charge of membership, attendance o, the records of the organization concerned Disclosure under this subsection is not required if undisclosed participation is permissible and authorized by this procedure

2 Disclosure may be made by the DoD intelligence component involved, an authorized DoD official, or by another component of the Intelligence Community that is otherwise authorized to take such action on behalf of the DoD intelligence component concerned

Part 11
PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES

A APPLICABILITY

This procedure applies to contracting or other arrangements with United States persons for the procurement of goods and services by DoD intelligence components within the United States and with contractors abroad who are US persons This procedure does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions The latter situation is governed by Procedure 10

B PROCEDURES

1 Contracts with academic institutions DoD intelligence components may enter into a contract for goods or services with an academic institution only if prior to the making of the contract, the intelligence component has disclosed to appropriate officials of the academic institution the fact of sponsorship by a DoD intelligence component

2 Contracts with commercial organizations, private institutions and individuals Contracting by or for a DoD intelligence component with commercial organizations, private institutions, or private individuals within the United States may be done without revealing the sponsorship of the intelligence component if

(a) The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities, or

(b) There is a written determination by the Secretary or the Under Secretary of a Military Department, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, or the Deputy Under Secretary of Defense (Policy) that the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned Requests by Army intelligence elements for authority to conceal such sponsorship will be submitted through command channels to HQDA (DAMI–CIC), WASH DC 20310

C EFFECTS OF NON–COMPLIANCE

No contract shall be void or voidable for failure to comply with this procedure

Part 12
PROCEDURE 12 PROVISIONS OF ASSISTANT TO LAW ENFORCEMENT AUTHORITIES

A APPLICABILITY

This procedure applies to the provision of assistant by DoD intelligence components to law enforcement authorities It incorporates the specific limitations on such assistant contained in E O 12333, (reference (a)), together with the general limitations and approval requirements of DoD Directive 5525 5, (reference (i)) (See AR 500–51)

B PROCEDURES

1 Cooperation with law enforcement authorities Consistent with the limitations contained in DoD Directive 5525 5, (reference (i)) and subsection B 2 , below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of

(a) Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities,

(b) Protecting DoD employees, information, property and facilities, and

(c) Preventing, detecting or investigating other violations of law

2 Types of permissible assistant DoD intelligence components may provide the following types of assistant to law enforcement authorities

(a) Incidentally–acquired information reasonably believed to indicate a violation of federal law shall be provided in accordance with the procedures adopted pursuant to section 1 7(a) of E O 1233 (reference (a)) Policy governing reporting and use of information concerning Federal crimes is found at procedure 15, section C 4

(b) Incidentally–acquired information reasonable believed to indicate a violation of state, local or foreign law may be provided in accordance with procedures adopted by the heads of DoD components,

(c) Specialized equipment and facilities may be provided to federal law enforcement authorities, and, where lives are endangered, to state and local law enforcement authorities, provided such assistant is consistent with, and has been approved by an official authorized pursuant to , enclosure 3 of DoD Directive 5525 5, (reference (i)), and

(d) Personnel who are employees of DoD intelligence components may be assigned to assist federal law enforcement authorities, and when lives are endangered, state and local law enforcement authorities; provided such use is consistent with, and has been approved by an official authorized pursuant to, enclosure 4 of DoD Directive 5525 5, (reference (i)) Such official shall ensure that the General Counsel of the providing DoD component concurs in such use

(e) Assistant may be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policy and applicable Status of Forces Agreements, provided, that DoD intelligence components may not request or participate in activities of such agencies undertaken against United States persons that would not be permitted such components under these procedures

Part 13
PROCEDURE 13. EXPERIMENTATION OF HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

A APPLICABILITY

This procedure applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a DoD intelligence component This procedure does not apply to experimentation on animal subjects

B EXPLANATION OF UNDEFINED TERMS

1 Experimentation in this context means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives

2 Experimentation is conducted on behalf of a DoD intelligence component if it is conducted under contract to that component or to another DoD component for the benefit of the intelligence component or at the request of such a component regardless of any existence of a contractual relationship

3 Human subjects in this context includes any person whether or not such person is a United States person

C PROCEDURES

1 Experimentation on human subjects conducted by or on behalf of a DoD intelligence component may be undertaken only with the informed consent of the subject, and in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects

2 DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the Secretary or Deputy Secretary of Defense, or the Secretary or Under Secretary of a Military Department, as appropriate Request for such approval submitted by Army intelligence components will be addressed through command channels to HQDA (DAMI–CIC), WASH DC 20310

Part 14
PROCEDURE 14 EMPLOYEE CONDUCT

A APPLICABILITY

This procedure sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this Regulation and other applicable policy It also provides that DoD intelligence components shall ensure, as appropriate, that these policies and guidelines are made known to their employees

B PROCEDURES

1 Employee responsibilities Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence components by law, Executive Order, including EO 12333 (reference (a)), and applicable DoD directives

2 Familiarity with restrictions

(a) Each DoD intelligence component shall familiarize its personnel with the provisions of Executive Order 12333, (reference (a)), this Regulation, and any instructions implementing this Regulation which apply to the operations and activities of such component At a minimum, such familiarization shall contain

(1) Applicable portions of Procedures 1 through 4

(2) A summary of other procedures that pertain to collection techniques which are, or may be, employed by the DoD intelligence component concerned, and

(3) A statement of individual employee reporting responsibility under Procedure 15

(b) The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD (IO)), and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect which achieve the objectives set forth in paragraph B 2 a , above

3 Responsibilities of the heads of DoD components The heads of DoD Comps that constitute, or contain, DoD intelligence components (The Secretary of the Army) shall

(a) Ensure that all proposals for intelligence activities which may be unlawful, in whole or in part, or may be contrary to applicable Executive Branch or DoD policy are referred to the General Counsel responsible for such component

(b) Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15

(c) Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder

(d) In any case involving serious or continuing breaches of security by either DoD or non-DoD employees, recommend to the Secretary of Defense appropriate investigative actions

(e) Ensure that the General Counsel and Inspector General with responsibility for the component (The Army General Counsel and the DA Inspector General), as well as the General Counsel, DoD, and the ATSD (IO), (and the intelligence oversight officer, office of the ACSI, HQDA) have access to all information concerning the intelligence activities of that component necessary to perform their oversight responsibilities

(f) Ensure that employees cooperate fully with the Intelligence Oversight Board and its representatives

Part 15
PROCEDURE 15 IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE ACTIVITIES

A APPLICABILITY

This procedure provides for the identification, investigation, and reporting of questionable intelligence activities

B EXPLANATION OF UNDEFINED TERMS

1 The term "questionable activity," as used herein, refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive Order or Presidential directive including E O 12333, reference (a)), or applicable DoD policy including this Regulation

2 The terms "General Counsel" and "Inspector General " as used herein, refer, unless otherwise specified, to any General Counsel or Inspector General with responsibility for one or more DoD intelligence components Unless otherwise indicated, the term "Inspector General " shall also include the ATSD (IO) For the purposes of this procedure the terms refer to the Army General Counsel and the DA Inspector General

C PROCEDURES

1 Identification

(a) Each employee shall report any questionable activities to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the DoD General Counsel or the ATSD (IO)

(1) Questionable activities will be reported by electrical message through command channels to HQDA (DAMI–CIC), WASH DC 20310, as soon as possible (but in any event not later than five days of discovery) Reports will include the following

a Description of the nature of the questionable activity

b Date, time, and location of occurrence

c Individual or unit responsible for the questionable activity

d Summary of the incident to include references to particular portions of this regulation

e Status of the investigation of the incident

(2) Employees are encouraged to submit such reports through command channels, however, if the employee desires, reports of questionable activity may be sent directly to the following The ACSI, HQDA, the Office of The Inspector General, HQDA, or the Office of the Army General Counsel, WASH DC 20310

(b) Inspectors General, as part of their inspection of DoD intelligence components, and General Counsels, as part of their oversight responsibilities shall seek to determine if such components are involved in any questionable activities If such activities have been or are being undertaken, the matter shall be investigated under subsection C 2 below If such activities have been undertaken but were not reported, the Inspector General shall also ascertain the reason for such failure and recommend appropriate corrective action

(c) Inspectors General, as part of their oversight responsibilities, shall, as appropriate, ascertain whether any organization, staffs, or offices within their respective jurisdiction but not otherwise specifically identified as DoD intelligence components, are being used for foreign intelligence or counterintelligence purposes to which Part 2 of E O 12333, (reference (a)), applies, and, if so, shall ensure that activities of such components are in compliance with this Regulation and applicable DoD policy

(d) Inspectors General, as part of their inspection of DoD intelligence components, shall ensure that procedures exist within such components for the reporting of questionable activities, and that employees of such components are aware of their responsibilities to report such activities

2 Investigation

(a) Each report of a questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy

(1) Initial investigation will be conducted in an expeditious manner by the command which reported the questionable activity

(2) Within 30 days of the initial report, the command will forward a final report through command channels to HQDA (DAMI–CIC), WASH DC 20310 for submission to the DA Inspector General and the Army General Counsel The report will be reviewed by the supporting judge advocate, it will include the following

a Results of the investigation

b Disciplinary or corrective action taken or contemplated

(3) If the investigation cannot be completed within 30 days from the date of the initial report, a status report will be submitted, the report will provide the reasons for the delay and an estimated date of completion Status reports will be forwarded every 30 days until the investigation is completed Except in extraordinary circumstances, investigations will be completed and a final report sent within 60 days from the date of the original report

(4) Pursuant to AR 335–15, paragraph 7–2r, the above reports are exempt from the requirement for a Requirements Control Symbol

(b) When appropriate, questionable activities reported to a General Counsel shall be referred to the corresponding Inspector General for investigation, and if reported to the Inspector General, shall be referred to the corresponding General Counsel to determine whether the activity is legal and consistent with applicable policy Reports made to the DoD General Counsel or the ATSD (IO) may be referred, after consultation between these officials, to the appropriate Inspector General and General Counsel for investigation and evaluation

(c) Investigations shall be conducted expeditiously The officials

responsible for these investigations may, in accordance with established procedures, obtain assistant from within the component concerned, or from other DoD components, when necessary, to complete such investigations in a timely manner

(d) To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation

3 Reports

(a) Each Counsel and Inspector General shall report immediately to General Counsel, DoD, and the ASTD questionable activities of a serious nature

(b) Each General Counsel and Inspector General shall submit to the ATSD (IO) a quarterly report described those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive Order or Presidential directive, or applicable DoD policy, and actions taken with respect to such activities The reports shall also include significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system Separate, joint, or consolidated reports may be submitted These reports should be prepared in accordance with DoD Directive 5000 11, (reference (j))

(1) The DA Inspector General will prepare the Quarterly Oversight Activities Report for the signature of The Inspector General and the Army General Counsel The report will be forwarded not later than 30 days following the end of each quarter

(2) To assist in preparing this report, the ACSI, HQDA, Commanding General, INSCOM, CINCUSAREUR, Commanding General, US Army Forces Command (FORSCOM), and the Commanding General, EUSA, will provided contributions not later than 15 days following the end of the quarter These reports will be forwarded through HQDA (DAMI–CIC), WASH DC 20310

(3) The quarterly reports will include the following

a Description of significant oversight activities undertaken during the quarter

b Identification of unlawful or improper activities discovered or reported

c Suggestions for improvements of the oversight system

(4) Pursuant to AR 335–15, paragraph 7–2r, these quarterly reports are exempt from the requirement for a Requirements Control Symbol

(c) All reports made pursuant to subsections 3 a and b above, which involve a possible violation of federal criminal law shall be considered by the General Counsel concerned in accordance with the procedures adopted pursuant to section 1 7(a) of E O 12333 (reference (a))

(d) The General Counsel, DoD, and the ATSD (IO) may review the findings of other General Counsels and Inspector Generals with respect to questionable activities

(e) The ATSD (IO) and the General Counsel, DoD, shall report in a timely manner to the White House Intelligence Oversight Board all activities that come to their attention that are reasonably believed to be illegal or contrary to Executive Order or Presidential directive They will also advise appropriate officials of the Office of the Secretary of Defense of such activities

(f) These reporting requirements are exempt from formal approval and licensing in accordance with subsection VII G of enclosure 3 to DoD Directive 5000 19 (reference (k))

4 Reporting and use of information concerning Federal crimes

This section implements section 1 7(a) of Executive Order 12333, (reference (a))

(a) Any member or employee of an Army intelligence component will report immediately (through command channels if possible) any facts and circumstances that tend to show the following

(1) That a member or employee of a DA intelligence component may have violated any Federal statute

(2) That any other person may have violated a Federal criminal statute in one of the following categories

a Crimes involving intentional infliction of threat of death or serious physical harm

b Crimes likely to impact on the national security, defense, or foreign relations of the United States

c Crimes involving foreign interference with the integrity of US governmental institutions or processes

d Crimes that appear to have been committed by or on behalf of a foreign power or in connection with international terrorist activity

e Any conspiracy or attempt to commit a crime reportable under categories (a) through (d) above

(b) The intelligence component receiving the report will report all available facts by electrical message to HQDA WASH DC// DAMI–CIC// and to USACIDC when required by AR 195–2, within 5 days after discovery

(c) Questions involving the scope of this reporting requirement should be addressed to the legal advisor of the intelligence component receiving the report of possible criminal conduct

(d) The office of the ACSI, HQDA, will transmit reports pursuant to this section the Army General Counsel, with recommendations concerning the following

(1) The need for the scope of further inquiry

(2) Whether the allegations are without basis

(3) Whether the crime involved is one against property and involving less than $500

(4) Whether the offense is of such a minor nature that no further investigation is necessary and only an oral report to the Attorney General is required

(5) Whether further investigation or prosecution of the matter would or might result in a public disclosure of classified information or intelligence sources or methods or would jeopardize the security of ongoing intelligence operations (Where security considerations mandate, names in reports may be identified as "John Doe #_____", the true identity of such persons will be provided when so requested by the Army General Counsel)

(e) Reports received pursuant to this section will be reviewed and reported by the Army General Counsel under procedures adopted by the Department of Justice

(f) For purposes of this section the term "employee" is defined as

(1) A military member, employee, or contract employee of an intelligence component

(2) Former members and employees for purposes of offenses committed during their employment

(3) Former members and employees for offenses involving violation of section 207, title 18, United States Code (18 USC 207)

Appendix A
Definitions

1. Administrative purposes.

Information is collected for "administrative purposes" when it is necessary for the administration of the component concerned but is not collected directly in performance of the intelligence activities assigned such components Examples include information relating to the past performance of potential contractors, information to enable such components to discharge their public affairs and legislative duties, including the maintenance of correspondence files, the maintenance of employee personnel and training records, and training materials or documents produced at training facilities

2 Available publicly

Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public In this context, the 'general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public

3 Communications security.

Protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such telecommunications

4 Consent

The agreement by a person or organization to permit DoD intelligence components to take particular action that affect the person or organization Consent may be oral or written unless a specific form of consent is required by a particular procedure Consent may be implied if adequate notice is provided that a particular action (such as entering a building) carries with it the presumption of consent to an accompanying action (such as search of briefcases) (Questions regarding what is adequate notice in particular circumstances should be referred to the legal office responsible for advising the DoD intelligence component concerned)

5 Counterintelligence

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons. or international terrorist activities, but not including personnel physical document, or communications security programs

6 Counterintelligence investigation

Includes inquires and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts

7 DoD Component

Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chief of Staff, the Unified and Specified Commands, and the Defense Agencies For the purposes of this regulation, the head of the DoD Component is the Secretary or Under Secretary of the Army

8. DoD intelligence components.

Include the following organizations

a The National Security Agency/Central Security Service

b The Defense Intelligence Agency

c The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs

d The assistant Chief of Staff for Intelligence, Army General Staff

e The Office of Naval Intelligence

f The Assistant Chief of Staff, Intelligence, United States Air Force

g The Army Intelligence and Security Command

h The Naval Intelligence Command

i The Naval Security Group Command

j The Director of Intelligence, U S Marine Corps

k The Air Force Intelligence Service

l The Electronic Security Command, United States Air Force

m The counterintelligence elements of the Naval Investigative Service

n The counterintelligence elements of the Air Force Office of Special Investigations

o The 650th Military Intelligence Group, SHAPE

p Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E O 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation Included in this subcategory are the following intelligence units that support unified or specified commands, intelligence staff offices supporting military commanders at all echelons including their subordinate intelligence units and offices, and other DA components performing intelligence activities as that term is defined at paragraph 13

9 Electronic surveillance

Acquisition of a non–public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter (electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978, (reference b))) Pen register organizations are included within the term electronic surveillance

10 Employee

A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency

11 Foreign intelligence.

Information relating to the capabilities, intentions, and activities of foreign powers, organizations, and persons, but not including counterintelligence except for information on international terrorist activities

12. Foreign power

Any foreign government (regardless of whether recognized by the United States), foreign–based political party (or faction thereof), foreign military force, foreign–based terrorist group, or any organization composed, in major part, of any such entity or entities

13 Intelligence Activities.

Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a))

14. Intelligence Community and an agency of or within the Intelligence Community

Refers to the following organizations

a The Central Intelligence Agency (CIA)

b The National Security Agency (NSA)

c The Defense Intelligence Agency (DIA)

d The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs

e The Bureau of Intelligence and Research of the Department of State

f The intelligence elements of the Army, Navy, Air Force and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy

g The staff elements of the Office of the Director of Central Intelligence

15 International Narcotics Activities

Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with title 21, United States Code, Sections 811 and 812

16 Intelligence Terrorist Activities

Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the local in which the perpetrators operate or seek asylum

17 Lawful Investigation

An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction, if it is conducted by a DoD component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security), and if the investigation is conducted in accordance with applicable law and policy, including E O 12333 and this Regulation

18 Law Enforcement Activities

Activities undertaken for the purpose of detecting violations of law or to locate and apprehend persons who violate the law This includes activities to enforce the Uniform Code of Military Justice

19 Personnel security

Measures designed to insure that persons employed, or being considered for employment, in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security

20 Personnel security investigation.

a An inquiry into the activities of a person granted access to intelligence or other classified information, or a person who is being considered for access to intelligence or other classified information, including persons who are granted or may be granted access to facilities of DoD intelligence components, or a person to be assigned or retained in a position with sensitive duties The investigation is designed to develop information pertaining to the suitability, eligibility and trustworthiness of the individual with respect to loyalty, character, emotional stability and reliability

b Inquiries and other activities directed against DoD employees or members of a military service to determine the facts of possible voluntary or involuntary compromise of classified information by them

c The collection of information about or from military personnel in the course of tactical training exercises for security training purposes

21 Physical security.

The physical measures taken to prevent unauthorized access to, and prevent the damage or loss of, equipment, facilities, material and documents, and measures undertaken to protect DoD personnel from physical threats to their safety

22. Physical security investigation.

All inquiries, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security, and all inquiries and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property

23. Reasonable belief.

A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold belief Reasonable belief must rest on facts and circumstances that can be articulated, "hunches" or intuitions are not sufficient Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion with someone unfamiliar with foreign intelligence or counterintelligence work might not

24. Signals Intelligence

A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination

25 Special Activities

Activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the US Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence US political processes, public opinion, or media, and do not include diplomatic activities or the collection of production of intelligence or related-support functions

26 United States

When used to describe a place, the term shall include the territories under the sovereignty of the United States

27 United States person

a The term "United States person" means

(1) A United States citizen,

(2) An alien known by the DoD intelligence component concerned to be a permanent resident alien,

(3) An unincoporated association substantially composed of United States citizens or permanent resident aliens,

(4) A corporation incorporated intelligence the United States, except for a corporation directed and controlled by a foreign government or governments A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated intelligence the United States, is not a United States person

b A person or organization outside the United States shall be presumed not to be a us person unless specific information to the contrary is obtained An alien in the United States shall be presumed

not to be a United States person unless specific information to the contrary is obtained

c A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence

Appendix B
Extract from "The Agreement between the Deputy Secretary of Defense and Attorney General, April 5, 1979"

Section 6 DELINEATION OF RESPONSIBILITY FOR CI INVESTIGATIONS Responsibility for CI investigations shall be apportioned between the FBI and the military CI services of the DoD as follows

a All investigations of violations of the Atomic Energy Act of 1946, which might constitute a CI investigation as defined herein, shall be the responsibility of the FBI, regardless of the status or location of the subjects of such investigations

b Except as provided by paragraph c(2) herein, all CI investigations of foreign nationals undertaken within the United States shall be the responsibility of the FBI

c CI investigations within the United States shall be conducted in accordance with the following jurisdictional guidelines

(1) Except as provided herein, investigations of all civilians, including DoD civilian personnel, shall be the responsibility of the FBI,

(2) Investigations of US military personnel on active duty shall be the responsibility of the CI service of the appropriate military department,

(3) Investigations of related military personnel, active and inactive reservists, and National Guard members shall be the responsibility of the FBI, provided, however, that investigations of actions which took place while the subject of the investigation was, or is, on active military duty shall be conducted by the CI service of the appropriate military department, and,

(4) Investigations of private contractors of the DoD and their employees, shall be the responsibility of the FBI. Provided, however, that nothing contained in this paragraph shall prevent the military CI services of the DoD, in a manner consistent with applicable law and Executive Branch policy, from undertaking

(a) In those cases where the FBI chooses to waive investigative jurisdiction, investigative actions which are necessary to establish or refute the factual basis required for an authorized administrative action, to protect the security of its personnel, information, activities, and installations, or

(b) To provide assistant to the FBI in support of any CI investigation for which the FBI is herein assigned responsibility

d CI investigations outside the United States shall be conducted in accordance with the following guidelines

(1) Investigations of military personnel on active duty shall be the responsibility of the military CI services of the DoD

(2) Investigations of current civilian employees, their dependents, and the civilian dependents of active duty military personnel shall be the responsibility of the military CI services, unless such responsibility is otherwise assigned pursuant to agreement with the host government, US law or Executive directive

(3) Investigations of retired military personnel, active and inactive reservists, National Guard members, private contractors and their employees, and other US persons, who permanently reside in such locations, shall be undertaken in consultation with the FBI, CIA, and host government as appropriate, Provided, however, that nothing contained in this paragraph shall prevent the military CI services of the DoD, in a manner consistent with applicable law and Executive Branch policy from undertaking

(a) Investigative actions which are necessary to establish or refute the factual basis required for an authorized administrative action, to protect the security of its personnel, information, activities, and installations, or

(b) To provide assistant to the FBI or security service of a host government in support of CI investigations outside the United States for which DoD is not herein assigned investigative responsibility

Appendix C
References to Army Implementation of DoD 5240.1–R

Section I
Required Publications

AR 190–13
The Army Physical Security Program Cited in procedure 2, section C 7

AR 190–52
Countering Terrorism and Other Major Disruptions on Military Installations Cited in procedure 2, section C 3 c , C 4 a , C 7 , C 7 , and C 11

AR 195–2
Criminal Investigation Activities Cited in procedure 1, section A 3, and procedure 15, section C6

AR 335–15
Management Information Control System Cited in procedure 15, sections C 2 a (4) and C 3 b (4)

AR 340–2
Maintenance and Disposition of Records in TOE units of the Active Army, the Army Reserve, and the National Guard Cited in procedure 3, section D 2

AR 340–18
The Army Functional Files System Cited in procedure 3, section D 2

AR 380–13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations Cited in the applicability statement on the title page

AR 380–53
Telephone Communications Security Monitoring Cited in procedure 2, section C 9, and procedure 5, part 7, section A

AR 381–12
Subversion and Espionage Directed Against US Army (SAEDA) Cited in procedure 1, section B, and procedure 2, sections C 4a , C 7 and C 8

AR 381–20
US Army Counterintelligence (CI) Activities Cited in procedure 1, sections A 3 and B, and procedure 2, sections C 7 and C 8

AR 381–45
Investigative Records Repository (IRR) Cited in procedure 3, section D 2

AR 381–47
(S) (US Army Offensive Counterintelligence Operations (Short Title OFCO) (U) Cited in paragraph B–3

AR 500–51
Support to Civilian Law Enforcement Cited in procedure 12, section A

AR 604–5
Clearance of Personnel for Access to Classified Defense Information and Material Cited in procedure 2, section C 8

DoD 4525.6–M
DoD Postal Manual Cited In procedure 4525 6–M 8, sections C 1 a and C 3 a

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 10–5
Department of the Army

AR20–1
Inspector General Activities and Procedures

AR 27–10
Military Justice

AR 195–1
Army Criminal Investigation Program

AR 340–21–5
The Army Privacy Program System Notices and Exemption Rules for Intelligence, Security, Military Police, and Mapping Functions

AR 380–5
Department of the Army Information Security Program

AR 381–1
Control of Dissemination of Intelligence Information

AR 600–50
Standards of Conduct for Department of the Army Personnel

Section III
Related Publications

Executive Order 12333
United States Intelligence Activities December 4, 1981

Public Law 95–511
Foreign Intelligence Surveillance Act of 1978

DoD Directive 5200 29
DoD Technical Surveillance Countermeasures (TSCM) Survey Program February 12, 1975

Title 18
United States Code, Chapters 105 and 119

Public Law 73–416
Communications Act of 1934, Section 605

Title 10
United States Code, Sections 801–840, Uniform Code of Military Justice

Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979 (App B)

Executive Order 12198
Prescribing Amendments to the Manual for Courts Martial United States 1969, March 12, 1980

DoD Directive 5525 5
DoD Cooperation with Civilian Law Enforcement Officials March 22, 1982

DoD Directive 5000 11
Data Elements and Data Codes Standardization Program December 7, 1964

DoD Directive 5000.19
Policies for the Management and Control of Information Requirements March 12, 1976

Appendix D
Part II, Executive Order 12333
Conduct of Intelligence Activities

2–1. Need.
Accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents is essential to informed decision making in the areas of national defense and foreign relations Collections of such information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded

2–2 Purpose
This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conduct by foreign powers Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency

2–3 Collection of Information
Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order Those procedures shall permit collection, retention and dissemination of the following types of information

a Information that is publicly available or collected with the consent of the person concerned,

b Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons,

c Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation,

d Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations,

e Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure Collection within the United States shall be undertaken by the FBI except that other agencies of Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting,

f Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility,

g Information arising out of a lawful personnel, physical or communications security investigation,

h Information acquired by overhead reconnaissance not directed at specific United States persons,

i Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws, and

j Information necessary for administrative purposes

In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community, for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it

2–4 Collection Techniques

Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, h surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes These procedures shall authorize

a The CIA to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance,

b Unconsented physical searches in the United States by agencies other than the FBI, except for

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers and

(2) Searches by CIA of personal property of non–United States persons lawfully in its possession

c Physical surveillance of a United States person in the United States by agencies other than the FBI, except for

(1) Physical surveillance of present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting, and

(2) Physical surveillance of a military person employed by a nonintelligence element of a military service

d Physical surveillance of a United States person abroad to collect foreign intelligence except to obtain significant information that cannot reasonably be acquired by other means

2–5 Attorney General Approval

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with the Act, as well as this Order

2–6 Assistant to Law Enforcement Authorities

Agencies within the Intelligence Community are authorized to

a Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community,

b Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities,

c Provide specialized equipment, technical knowledge, or assistant of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies Provisions of assistant by expert personnel shall be approved in each case by the General Counsel of the providing agency, and

d Render any other assistant and cooperation to law enforcement authorities not precluded by applicable law

2–7 Contracting.

Agencies within the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized academic institutions may be undertaken only with the consent of appropriate officials of the institution

2–8 Consistency With Other Laws.

Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States

2–9 Undisclosed Participation in Organizations Within the United States

No one acting on behalf of agencies within the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any agency within the Intelligence Community without disclosing his intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the agency concerned and approved by the Attorney General Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the agency head or designee No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where

a The participation is undertaken on behalf of the FBI in the course of a lawful investigation, or

b The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power

2–10 Human Experimentation

No agency within the Intelligence Community shall sponsor, contract for or conduct research on human subjects except in accordance with guideline issued by the Department of Health and Human Services The subject's informed consent shall be documented as required by those guidelines

2–11 Prohibition on Assassination

No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination

2–12 Indirect Participation

No agency of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN.	030887-000
DATE:	06-15-98
TIME.	14:58:35
PAGES SET.	28

DATA FILE.	a381.fil
DOCUMENT:	AR 381-10
DOC STATUS:	NEW PUBLICATION