

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

APPENDIX 4 MILITARY SUPPORT TO LAW ENFORCEMENT

Appendix 4-1: 18 U.S.C. § 1385 - The Posse Comitatus Act (PCA)

18 U.S.C. §1385 (2002)

Crimes and Criminal Procedure

Sec. 1385 Use of Army and Air Force as Posse Comitatus

Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.

Source

(Added Aug. 10, 1956, ch. 1041, Sec. 18(a), 70A Stat. 626; amended Pub. L. 86-70, Sec. 17(d), June 25, 1959, 73 Stat. 144; Pub. L. 103-322, title XXXIII, Sec. 330016(1)(L), Sept. 13, 1994, 108 Stat. 2147.)

Historical and Revision Note

<u>Revised Section</u>	<u>Source (U.S. Code)</u>	<u>Source (Statutes at Large)</u>
------------------------	---------------------------	-----------------------------------

1385	10:15.	June 18, 1878, ch. 263, Sec. 15, 20 Stat. 152; Mar. 3, 1899, ch. 429, Sec. 363 (proviso); added June 6, 1900, ch. 786, Sec. 29 (less last proviso), 31 Stat. 330.
------	--------	---

This section is revised to conform to the style and terminology used in title 18. It is not enacted as a part of title 10, United States Code, since it is more properly allocated to title 18.

Amendments

1994 - Pub. L. 103-322 substituted "fined under this title" for "fined not more than \$10,000".

1959 - Pub. L. 86-70 struck out provisions which made section inapplicable in Alaska.

Section Referred to in Other Sections

This section is referred to in section 831 of this title.

UPDATE: None

Appendix 4-2: 10 U.S.C. §§ 371-382 - Military Support to Civilian Law Enforcement Agencies

10 U.S.C. § 371, *et seq.* (2002)

Military Support for Civilian Law Enforcement Agencies

Section 371. Use of information collected during military operations

(a) The Secretary of Defense may, in accordance with other applicable law, provide to Federal, State, or local civilian law enforcement officials any information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

(b) The needs of civilian law enforcement officials for information shall, to the maximum extent practicable, be taken into account in the planning and execution of military training or operations.

(c) The Secretary of Defense shall ensure, to the extent consistent with national security, that intelligence information held by the Department of Defense and relevant to drug interdiction or other civilian law enforcement matters is provided promptly to appropriate civilian law enforcement officials.

Section 372. Use of military equipment and facilities

(a) In General. - The Secretary of Defense may, in accordance with other applicable law, make available any equipment (including associated supplies or spare parts), base facility, or research facility of the Department of Defense to any Federal, State, or local civilian law enforcement official for law enforcement purposes.

(b) Emergencies Involving Chemical and Biological Agents. - (1) In addition to equipment and facilities described in subsection (a), the Secretary may provide an item referred to in paragraph (2) to a Federal, State, or local law enforcement or emergency response agency to prepare for or respond to an emergency involving chemical or biological agents if the Secretary determines that the item is not reasonably available from another source. The requirement for a determination that an item is not reasonably available from another source does not apply to assistance provided under section 382 of this title pursuant to a request of the Attorney General for the assistance.

(2) An item referred to in paragraph (1) is any material or expertise of the Department of Defense appropriate for use in preparing for or responding to an emergency involving chemical or biological agents, including the following:

- (A) Training facilities.
- (B) Sensors.
- (C) Protective clothing.
- (D) Antidotes.

Section 373. Training and advising civilian law enforcement officials

The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available -

(1) to train Federal, State, and local civilian law enforcement officials in the operation and maintenance of equipment, including equipment made available under section 372 of this title; and

(2) to provide such law enforcement officials with expert advice relevant to the purposes of this chapter.

Section 374. Maintenance and operation of equipment

(a) The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available for the maintenance of equipment for Federal, State, and local civilian law enforcement officials, including equipment made available under section 372 of this title.

(b)(1) Subject to paragraph (2) and in accordance with other applicable law, the Secretary of Defense may, upon request from the head of a Federal law enforcement agency, make Department of Defense personnel available to operate equipment (including equipment made available under section 372 of this title) with respect to -

(A) a criminal violation of a provision of law specified in paragraph (4)(A);

(B) assistance that such agency is authorized to furnish to a State, local, or foreign government which is involved in the enforcement of similar laws;

(C) a foreign or domestic counter-terrorism operation; or

(D) a rendition of a suspected terrorist from a foreign country to the United States to stand trial.

(2) Department of Defense personnel made available to a civilian law enforcement agency under this subsection may operate equipment for the following purposes:

(A) Detection, monitoring, and communication of the movement of air and sea traffic.

(B) Detection, monitoring, and communication of the movement of surface traffic outside of the geographic boundary of the United States and within the United States not to exceed 25 miles of the boundary if the initial detection occurred outside of the boundary.

(C) Aerial reconnaissance.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

(D) Interception of vessels or aircraft detected outside the land area of the United States for the purposes of communicating with such vessels and aircraft to direct such vessels and aircraft to go to a location designated by appropriate civilian officials.

(E) Operation of equipment to facilitate communications in connection with law enforcement programs specified in paragraph

(4)(A).

(F) Subject to joint approval by the Secretary of Defense and the Attorney General (and the Secretary of State in the case of a law enforcement operation outside of the land area of the United States) -

(i) the transportation of civilian law enforcement personnel along with any other civilian or military personnel who are supporting, or conducting, a joint operation with civilian law enforcement personnel;

(ii) the operation of a base of operations for civilian law enforcement and supporting personnel; and

(iii) the transportation of suspected terrorists from foreign countries to the United States for trial (so long as the requesting Federal law enforcement agency provides all security for such transportation and maintains custody over the suspect through the duration of the transportation).

(3) Department of Defense personnel made available to operate equipment for the purpose stated in paragraph (2)(D) may continue to operate such equipment into the land area of the United States in cases involving the pursuit of vessels or aircraft where the detection began outside such land area.

(4) In this subsection:

(A) The term "Federal law enforcement agency" means a Federal agency with jurisdiction to enforce any of the following:

(i) The Controlled Substances Act (21 U.S.C. 801 et seq.) or the Controlled Substances Import and Export Act (21 U.S.C. 951 et seq.).

(ii) Any of sections 274 through 278 of the Immigration and Nationality Act (8 U.S.C. 1324-1328).

(iii) A law relating to the arrival or departure of merchandise (as defined in section 401 of the Tariff Act of 1930 (19 U.S.C. 1401) into or out of the customs territory of the United States (as defined in general note 2 of the Harmonized Tariff Schedule of the United States) or any other territory or possession of the United States.

(iv) The Maritime Drug Law Enforcement Act (46 U.S.C. App. 1901 et seq.).

(v) Any law, foreign or domestic, prohibiting terrorist activities.

(B) The term "land area of the United States" includes the land area of any territory, commonwealth, or possession of the United States.

(c) The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available to any Federal, State, or local civilian law enforcement agency to operate equipment for purposes other than described in subsection (b)(2) only to the extent that such support does not involve direct participation by such personnel in a civilian law enforcement operation unless such direct participation is otherwise authorized by law.

Section 375. Restriction on direct participation by military personnel

The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.

Section 376. Support not to affect adversely military preparedness

Support (including the provision of any equipment or facility or the assignment or detail of any personnel) may not be provided to any civilian law enforcement official under this chapter if the provision of such support will adversely affect the military preparedness of the United States. The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that the provision of any such support does not adversely affect the military preparedness of the United States.

Section 377. Reimbursement

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

(a) To the extent otherwise required by section 1535 of title 31 (popularly known as the "Economy Act") or other applicable law, the Secretary of Defense shall require a civilian law enforcement agency to which support is provided under this chapter to reimburse the Department of Defense for that support.

(b) An agency to which support is provided under this chapter is not required to reimburse the Department of Defense for such support if such support -

(1) is provided in the normal course of military training or operations; or

(2) results in a benefit to the element of the Department of Defense providing the support that is substantially equivalent to that which would otherwise be obtained from military operations or training.

Section 378. Nonpreemption of other law

Nothing in this chapter shall be construed to limit the authority of the executive branch in the use of military personnel or equipment for civilian law enforcement purposes beyond that provided by law before December 1, 1981.

Section 379. Assignment of Coast Guard personnel to naval vessels for law enforcement purposes

(a) The Secretary of Defense and the Secretary of Transportation shall provide that there be assigned on board every appropriate surface naval vessel at sea in a drug-interdiction area members of the Coast Guard who are trained in law enforcement and have powers of the Coast Guard under title 14, including the power to make arrests and to carry out searches and seizures.

(b) Members of the Coast Guard assigned to duty on board naval vessels under this section shall perform such law enforcement functions (including drug-interdiction functions) -

(1) as may be agreed upon by the Secretary of Defense and the Secretary of Transportation; and

(2) as are otherwise within the jurisdiction of the Coast Guard.

(c) No fewer than 500 active duty personnel of the Coast Guard shall be assigned each fiscal year to duty under this section. However, if at any time the Secretary of Transportation, after consultation with the Secretary of Defense, determines that there are insufficient naval vessels available for purposes of this section, such personnel may be assigned other duty involving enforcement of laws listed in section 374(b)(4)(A) of this title.

(d) In this section, the term "drug-interdiction area" means an area outside the land area of the United States (as defined in section 374(b)(4)(B) of this title) in which the Secretary of Defense (in consultation with the Attorney General) determines that activities involving smuggling of drugs into the United States are ongoing.

Section 380. Enhancement of cooperation with civilian law enforcement officials

(a) The Secretary of Defense, in cooperation with the Attorney General, shall conduct an annual briefing of law enforcement personnel of each State (including law enforcement personnel of the political subdivisions of each State) regarding information, training, technical support, and equipment and facilities available to civilian law enforcement personnel from the Department of Defense.

(b) Each briefing conducted under subsection (a) shall include the following:

(1) An explanation of the procedures for civilian law enforcement officials -

(A) to obtain information, equipment, training, expert advice, and other personnel support under this chapter; and

(B) to obtain surplus military equipment.

(2) A description of the types of information, equipment and facilities, and training and advice available to civilian law enforcement officials from the Department of Defense.

(3) A current, comprehensive list of military equipment which is suitable for law enforcement officials from the Department of Defense or available as surplus property from the Administrator of General Services.

(c) The Attorney General and the Administrator of General Services shall -

(1) establish or designate an appropriate office or offices to maintain the list described in subsection (b)(3) and to furnish information to civilian law enforcement officials on the availability of surplus military equipment; and

(2) make available to civilian law enforcement personnel nationwide, toll free telephone communication with such office or offices

Section 382. Emergency situations involving chemical or biological weapons of mass destruction

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

(a) In General. - The Secretary of Defense, upon the request of the Attorney General, may provide assistance in support of Department of Justice activities relating to the enforcement of section 175 or 2332c (FOOTNOTE 1) of title 18 during an emergency situation involving a biological or chemical weapon of mass destruction. Department of Defense resources, including personnel of the Department of Defense, may be used to provide such assistance if -

(FOOTNOTE 1) See References in Text note below.

(1) the Secretary of Defense and the Attorney General jointly determine that an emergency situation exists; and

(2) the Secretary of Defense determines that the provision of such assistance will not adversely affect the military preparedness of the United States.

(b) Emergency Situations Covered. - In this section, the term "emergency situation involving a biological or chemical weapon of mass destruction" means a circumstance involving a biological or chemical weapon of mass destruction -

(1) that poses a serious threat to the interests of the United States; and

(2) in which -

(A) civilian expertise and capabilities are not readily available to provide the required assistance to counter the threat immediately posed by the weapon involved;

(B) special capabilities and expertise of the Department of Defense are necessary and critical to counter the threat posed by the weapon involved; and

(C) enforcement of section 175 or 2332c (FOOTNOTE 1) of title 18 would be seriously impaired if the Department of Defense assistance were not provided.

(c) Forms of Assistance. - The assistance referred to in subsection (a) includes the operation of equipment (including equipment made available under section 372 of this title) to monitor, contain, disable, or dispose of the weapon involved or elements of the weapon.

(d) Regulations. - (1) The Secretary of Defense and the Attorney General shall jointly prescribe regulations concerning the types of assistance that may be provided under this section. Such regulations shall also describe the actions that Department of Defense personnel may take in circumstances incident to the provision of assistance under this section.

(2)(A) Except as provided in subparagraph (B), the regulations may not authorize the following actions:

(i) Arrest.

(ii) Any direct participation in conducting a search for or seizure of evidence related to a violation of section 175 or 2332c (FOOTNOTE 1) of title 18.

(iii) Any direct participation in the collection of intelligence for law enforcement purposes.

(B) The regulations may authorize an action described in subparagraph (A) to be taken under the following conditions:

(i) The action is considered necessary for the immediate protection of human life, and civilian law enforcement officials are not capable of taking the action.

(ii) The action is otherwise authorized under subsection (c) or under otherwise applicable law.

(e) Reimbursements. - The Secretary of Defense shall require reimbursement as a condition for providing assistance under this section to the extent required under section 377 of this title.

(f) Delegations of Authority. - (1) Except to the extent otherwise provided by the Secretary of Defense, the Deputy Secretary of Defense may exercise the authority of the Secretary of Defense under this section. The Secretary of Defense may delegate the Secretary's authority under this section only to an Under Secretary of Defense or an Assistant Secretary of Defense and only if the Under Secretary or Assistant Secretary to whom delegated has been designated by the Secretary to act for, and to exercise the general powers of, the Secretary.

(2) Except to the extent otherwise provided by the Attorney General, the Deputy Attorney General may exercise the authority of the Attorney General under this section. The Attorney General may delegate that authority only to the Associate Attorney General or an Assistant Attorney General and only if the Associate Attorney General or Assistant Attorney General to whom delegated has been designated by the Attorney General to act for, and to exercise the general powers of, the Attorney General.

(g) Relationship to Other Authority. - Nothing in this section shall be construed to restrict any executive branch authority regarding use of members of the armed forces or equipment of the Department of Defense that was in effect before September 23, 1996.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

UPDATES

Pub. L. 107-248

Section 374. New note added by Pub. L. 107-248, sec. 8058(a), 116 Stat. 1549.

Pub. L. 108-87

Section 374. New note added by Pub. L. 108-87, sec. 8057(a), 117 Stat. 1085.

Pub. L. 107-296

Section 379. Amended by Pub. L. 107-296, sec. 1704(b)(1), 116 Stat. 2314.

Appendix 4-3: DODD 5200.27 - Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

Department of Defense DIRECTIVE

NUMBER 5200.27
January 7, 1980

USD(P)

SUBJECT: Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

References:

- (a) DoD Directive 5200.27, subject as above, December 8, 1975 (hereby canceled)
- (b) [DoD Directive 5240.1](#), "Activities of DoD Intelligence Components that Affect U.S. Persons," November 30, 1979

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to establish for the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the Department of Defense.

2. APPLICABILITY AND SCOPE

2.1. Except as provided by paragraph 2.3., below, this Directive is applicable to the Office of the Secretary of Defense, Military Departments, Office of the Joint Chiefs of Staff, Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2.2. The provisions of this Directive encompass the acquisition of information concerning the activities of:

2.2.1. Persons and organizations, not affiliated with the Department of Defense, within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions; and

2.2.2. Non-DoD-affiliated U.S. citizens anywhere in the world.

2.3. This Directive is not applicable to DoD intelligence components as defined by DoD Directive 5240.1 (reference (b)).

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

2.4. Authority to act for the Secretary of Defense in matters in this Directive that require specific approval are delineated in enclosure 1.

3. POLICY

3.1. DoD policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with the Department of Defense, except in those limited circumstances where such information is essential to the accomplishment of the DoD missions outlined below.

3.2. Information-gathering activities shall be subject to overall civilian control, a high level of general supervision and frequent inspections at the field level.

3.3. Where collection activities are authorized to meet an essential requirement for information, maximum reliance shall be placed upon domestic civilian investigative agencies, Federal, State, and local.

3.4. In applying the criteria for the acquisition and retention of information established pursuant to this Directive, due consideration shall be given to the need to protect DoD functions and property in the different circumstances existing in geographic areas outside the United States. Relevant factors include:

3.4.1. The level of disruptive activity against U.S. Forces;

3.4.2. The competence of host-country investigative agencies;

3.4.3. The degree to which U.S. Military and host-country agencies exchange investigative information;

3.4.4. The absence of other U.S. investigative capabilities; and

3.4.5. The unique and vulnerable position of U.S. Forces abroad.

4. AUTHORIZED ACTIVITIES

The DoD Components are authorized to gather information essential to the accomplishment of the following defense missions:

4.1. Protection of DoD Functions and Property. Information may be acquired about activities threatening defense military and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies. Only the following types of activities justify acquisition of information under the authority of this paragraph:

4.1.1. Subversion of loyalty, discipline, or morale of DoD military or civilian personnel by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities.

4.1.2. Theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment, or records belonging to DoD units or installations.

4.1.3. Acts jeopardizing the security of DoD elements or operations or compromising classified defense information by unauthorized disclosure or by espionage.

4.1.4. Unauthorized demonstrations on Active or Reserve DoD installations.

4.1.5. Direct threats to DoD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DoD resources.

4.1.6. Activities endangering facilities that have classified defense contracts or that have been officially designated as key defense facilities.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

4.1.7. Crimes for which the Department of Defense has responsibility for investigating or prosecuting.

4.2. Personnel Security. Investigations may be conducted in relation to the following categories of persons:

4.2.1. Members of the Armed Forces, including retired personnel, members of the Reserve components, and applicants for commission or enlistment.

4.2.2. DoD civilian personnel and applicants for such status.

4.2.3. Persons having need for access to official information requiring protection in the interest of national defense under the DoD Industrial Security Program or being considered for participation in other authorized DoD programs.

4.3. Operations Related to Civil Disturbance. The Attorney General is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. Upon specific prior authorization of the Secretary of Defense or his designee, information may be acquired that is essential to meet operational requirements flowing from the mission assigned to the Department of Defense to assist civil authorities in dealing with civil disturbances. Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law enforcement capabilities of State and local authorities.

5. PROHIBITED ACTIVITIES

5.1. The acquisition of information on individuals or organizations not affiliated with the DoD will be restricted to that which is essential to the accomplishment of assigned DoD missions under this Directive.

5.2. No information shall be acquired about a person or organization solely because of lawful advocacy of measures in opposition to Government policy.

5.3. There shall be no physical or electronic surveillance of Federal, State, or local officials or of candidates for such offices.

5.4. There shall be no electronic surveillance of any individual or organization, except as authorized by law.

5.5. There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense, or his designee.

5.6. No DoD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information, the collection of which is authorized by this Directive without specific prior approval by the Secretary of Defense, or his designee. An exception to this policy may be made by the local commander concerned, or higher authority, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case a report will be made immediately to the Secretary of Defense, or his designee.

5.7. No computerized data banks shall be maintained relating to individuals or organizations not affiliated with the Department of Defense, unless authorized by the Secretary of Defense, or his designee.

6. OPERATIONAL GUIDANCE

6.1. Nothing in this Directive shall be construed to prohibit the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, or the violation of law, nor to prohibit keeping a record of such a report.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

6.2. Nothing in this Directive shall be construed to restrict the direct acquisition by overt means of the following information:

6.2.1. Listings of Federal, State, and local officials who have official responsibilities related to the control of civil disturbances. Such listings may be maintained currently.

6.2.2. Physical data on vital public or private installations, facilities, highways, and utilities, as appropriate, to carry out a mission assigned by this Directive.

6.3. Access to information obtained under the provisions of this Directive shall be restricted to Governmental Agencies that require such information in the execution of their duties.

6.4. Information within the purview of this Directive, regardless of when acquired, shall be destroyed within 90 days unless its retention is required by law or unless its retention is specifically authorized under criteria established by the Secretary of Defense, or his designee.

6.5. This Directive does not abrogate any provision of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979, nor preclude the collection of information required by Federal statute or Executive order.

7. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing regulations to the Deputy Under Secretary of Defense (Policy Review) within 120 days.

/S/
W. Graham Claytor, Jr.
Deputy Secretary of Defense

Enclosures - 1

E1. Delegation of Authority

E1. ENCLOSURE 1 DELEGATION OF AUTHORITY

E1.1.1. The Secretary of the Army is designated to authorize those activities delineated in paragraph 4.3., basic Directive. This authority may not be further delegated to other than the Under Secretary of the Army.

E1.1.2. The Deputy Under Secretary of Defense (Policy Review) (DUSD(PR)) is designated to authorize those activities delineated in paragraph 5.5., basic Directive, within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be delegated. The investigating DoD Component, prior to requesting approval for authorizations under this provision, shall coordinate prospective activities with the Federal Bureau of Investigation.

E1.1.3. The DUSD(PR) and the Secretaries of the Military Departments are designated to authorize those activities (delineated in paragraph 5.5., basic Directive) abroad¹ when membership of the civilian organization is reasonably expected to include a significant number of non-DoD-affiliated U.S. citizens. This authority may not be further delegated to other than the Under Secretaries of the Military Departments. When the Military Department Secretary or Under Secretary exercises this delegation of authority, the DUSD(PR) shall be advised promptly.

E1.1.4. The Secretaries of the Military Departments are designated to authorize in their Departments those activities delineated in paragraph 5.6., basic Directive, within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be further delegated to other than the Under Secretaries of the Military Departments.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

E1.1.5. The Secretaries of the Military Departments are designated to authorize in their Departments those activities (delineated in paragraph 5.6., basic Directive) abroad¹ when a significant number of non-DoD-affiliated U.S. citizens are expected to be present. This authority may be further delegated, in writing, as circumstances warrant, to an authorized designee. The DUSD(PR) will be notified immediately of such further delegations of authority. When the Secretary or Under Secretary of a Military Department or his designee exercises this delegated authority, the DUSD(PR) shall be advised promptly.

E1.1.6. The DUSD(PR) is designated to authorize those activities delineated in paragraphs 5.7. and 6.4., basic Directive. These authorities may not be further delegated.

¹ "Abroad" means "outside the United States, its territories, and possessions."

Appendix 4-4: DOD 5240.1-R - Procedures Governing the Activities of DOD Intelligence Components that Affect U.S. Persons

TITLE: DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons", 12/1982

SUMMARY: This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect United States persons. It implements DoD Directives 5260.1, 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 U.S. persons be governed by procedures issued by the agency head and approved by the Attorney General.

Source: http://www.dtic.mil/whs/directives/corres/pdf/52401r_1282/p52401r.pdf

APPENDIX 4: MILITARY SUPPORT
TO LAW ENFORCEMENT

DoD 5240 1-R



DEPARTMENT OF DEFENSE

**PROCEDURES GOVERNING THE
ACTIVITIES OF
DOD INTELLIGENCE COMPONENTS
THAT AFFECT UNITED STATES PERSONS**

DECEMBER 1982

UNDER SECRETARY OF DEFENSE FOR POLICY

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

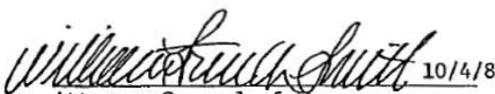
FOREWORD

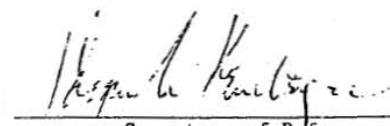
This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect United States persons. It implements DoD Directive 5240.1, and replaces the November 30, 1979 version of DoD Regulation 5240.1-R. It is applicable to all DoD intelligence components.

Executive Order 12333, "United States Intelligence Activities," stipulates that certain activities of intelligence components that affect U.S. 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.

 10/4/82
Attorney General of the
United States

 12/7/82
Secretary of Defense

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	2
TABLE OF CONTENTS	3
REFERENCES	6
DEFINITIONS	7
CHAPTER 1 - PROCEDURE 1. GENERAL PROVISIONS	13
C1.1. APPLICABILITY AND SCOPE	13
C1.2. SCOPE	13
C1.3. INTERPRETATION	14
C1.4. EXCEPTIONS TO POLICY	14
C1.5. AMENDMENT	14
CHAPTER 2 - PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS	15
C2.1. APPLICABILITY AND SCOPE	15
C2.2. EXPLANATION OF UNDEFINED TERMS	15
C2.3. TYPES OF INFORMATION THAT MAYBE COLLECTED ABOUT UNITED STATES PERSONS	16
C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS	18
C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES	18
CHAPTER 3 - PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS	20
C3.1. APPLICABILITY	20
C3.2. EXPLANATION OF UNDEFINED TERMS	20
C3.3. CRITERIA FOR RETENTION	20
C3.4. ACCESS AND RETENTION	21
CHAPTER 4 - PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS	22
C4.1. APPLICABILITY AND SCOPE	22
C4.2. CRITERIA FOR DISSEMINATION	22
C4.3. OTHER DISSEMINATION	23

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

TABLE OF CONTENTS, continued

	<u>Page</u>
CHAPTER 5 - PROCEDURE 5. ELECTRONIC SURVEILLANCE	24
C5.1. PART 1. ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES	24
C5.2. PART 2. ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES	25
C5.3. PART 3. SIGNALS INTELLIGENCE ACTIVITIES	28
C5.4. PART 4. TECHNICAL SURVEILLANCE COUNTERMEASURES	31
C5.5. PART 5. DEVELOPING, TESTING AND CALIBRATION OF ELECTRONIC EQUIPMENT	32
C5.6. PART 6. TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT	34
C5.7. PART 7. CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS	36
CHAPTER 6 - PROCEDURE 6. CONCEALED MONITORING	38
C6.1. APPLICABILITY AND SCOPE	38
C6.2. EXPLANATION OF UNDEFINED TERMS	38
C6.3. PROCEDURES	39
CHAPTER 7 - PROCEDURE 7. PHYSICAL SEARCHES	41
C7.1. APPLICABILITY AND SCOPE	41
C7.2. EXPLANATION OF UNDEFINED TERMS	41
C7.3. PROCEDURES	41
CHAPTER 8 - PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL	45
C8.1. APPLICABILITY	45
C8.2. EXPLANATION OF UNDEFINED TERMS	45
C8.3. PROCEDURES	46
CHAPTER 9 - PROCEDURE 9. PHYSICAL SURVEILLANCE	47
C9.1. APPLICABILITY	47
C9.2. EXPLANATION OF UNDEFINED TERMS	47
C9.3. PROCEDURES	47

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

TABLE OF CONTENTS, continued

	<u>Page</u>
CHAPTER 10 - PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS	49
C10.1. APPLICABILITY	49
C10.2. EXPLANATION OF UNDEFINED TERMS	49
C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION	50
C10.4. DISCLOSURE REQUIREMENT	53
CHAPTER 11 - PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES	54
C11.1. APPLICABILITY	54
C11.2. PROCEDURES	54
C11.3. EFFECT OF NONCOMPLIANCE	55
CHAPTER 12 - PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES	56
C12.1. APPLICABILITY	56
C12.2. PROCEDURES	56
CHAPTER 13 - PROCEDURE 13. EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES	58
C13.1. APPLICABILITY	58
C13.2. EXPLANATION OF UNDEFINED TERMS	58
C13.3. PROCEDURES	58
CHAPTER 14 - PROCEDURE 14. EMPLOYEE CONDUCT	60
C14.1. APPLICABILITY	60
C14.2. PROCEDURES	60
CHAPTER 15 - PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE ACTIVITIES	62
C15.1. APPLICABILITY	62
C15.2. EXPLANATION OF UNDEFINED TERMS	62
C15.3. PROCEDURES	62

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

REFERENCES

- (a) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (b) Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978"
- (c) DoD Directive 5200.29, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," February 12, 1975
- (d) Chapters 105 and 119 of title 18, United States Code
- (e) Public Law 73-416, "Communications Act of 1934," Section 605
- (f) Sections 801-840 of title 10, United States Code, "Uniform Code of Military Justice"
- (g) Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979
- (h) Executive Order 12198, "Prescribing Amendments to the Manual for Courts-Martial, United States, 1969," March 12, 1980
- (i) [DoD Directive 5525.5](#), "DoD Cooperation with Civilian Law Enforcement Officials," March 22, 1982
- (j) DoD Directive 5000.11, "Data Elements and Data Codes Standardization Program," December 7, 1964
- (k) DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

DL1. DEFINITIONS

DL1.1.1. 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 component. 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.

DL1.1.2. 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.

DL1.1.3. Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such telecommunications.

DL1.1.4. Consent. The agreement by a person or organization to permit DoD intelligence components to take particular actions 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.)

DL1.1.5. 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, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

DL1.1.6. Counterintelligence Investigation. Includes inquiries 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.

DL1.1.7. DoD Component. Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

DL1.1.8. DoD Intelligence Components. Include the following organizations:

DL1.1.8.1. The National Security Agency/Central Security Service.

DL1.1.8.2. The Defense Intelligence Agency.

DL1.1.8.3. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

DL1.1.8.4. The Assistant Chief of Staff for Intelligence, Army General Staff.

DL1.1.8.5. The Office of Naval Intelligence.

DL1.1.8.6. The Assistant Chief of Staff, Intelligence, U. S. Air Force.

DL1.1.8.7. The Army Intelligence and Security Command.

DL1.1.8.8. The Naval Intelligence Command.

DL1.1.8.9. The Naval Security Group Command.

DL1.1.8.10. The Director of Intelligence, U.S. Marine Corps.

DL1.1.8.11. The Air Force Intelligence Service.

DL1.1.8.12. The Electronic Security Command, U.S. Air Force.

DL1.1.8.13. The counterintelligence elements of the Naval Investigative Service.

DL1.1.8.14. The counterintelligence elements of the Air Force Office of Special Investigations.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

DL1.1.8.15. The 650th Military Intelligence Group, SHAPE.

DL1.1.8.16. 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.

DL1.1.9. Electronic Surveillance. Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic 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)).)

DL1.1.10. 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.

DL1.1.11. Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

DL1.1.12. 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.

DL1.1.13. Intelligence Activities. Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a)).

DL1.1.14. Intelligence Community and an Agency of Or Within the Intelligence Community. Refers to the following organizations:

DL1.1.14.1. The Central Intelligence Agency (CIA).

DL1.1.14.2. The National Security Agency (NSA).

DL1.1.14.3. The Defense Intelligence Agency (DIA).

APPENDIX 4: MILITARY SUPPORT
TO LAW ENFORCEMENT

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

DL1.1.14.4. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

DL1.1.14.5. The Bureau of Intelligence and Research of the Department of State.

DL1.1.14.6. The intelligence elements of the Army, the Navy, the Air Force and the Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.

DL1.1.14.7. The staff elements of the Office of the Director of Central Intelligence.

DL1.1.15. International Narcotics Activities. Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with Sections 811 and 812 of title 21, United States Code.

DL1.1.16. International 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 locale in which the perpetrators operate or seek asylum.

DL1.1.17. 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.

DL1.1.18. 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.

DL1.1.19. Personnel Security Investigation:

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

DL1.1.19.1. 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.

DL1.1.19.2. 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.

DL1.1.19.3. The collection of information about or from military personnel in the course of tactical training exercises for security training purposes.

DL1.1.20. Physical Security. The physical measures taken to prevent unauthorized access to, and prevent the damage or loss of, equipment, facilities, materiel and documents; and measures undertaken to protect DoD personnel from physical threats to their safety.

DL1.1.21. 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.

DL1.1.22. Reasonable Belief. A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the 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 and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not.

DL1.1.23. Signals Intelligence. A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

DL1.1.24. United States. When used to describe a place, the term shall include the territories under the sovereignty of the United States.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

DL1.1.25. United States Person

DL1.1.25.1. The term "United States person" means:

DL1.1.25.1.1. A United States citizen;

DL1.1.25.1.2. An alien known by the DoD intelligence component concerned to be a permanent resident alien;

DL1.1.25.1.3. An unincorporated association substantially composed of United States citizens or permanent resident aliens;

DL1.1.25.1.4. A corporation incorporated in 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 in the United States, is not a United States person.

DL1.1.25.2. A person or organization outside the United States shall be presumed not to be a United States 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.

DL1.1.25.3. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C1. CHAPTER 1

PROCEDURE 1. GENERAL PROVISIONS

C1.1. APPLICABILITY AND SCOPE

C1.1.1. These procedures apply only to "DoD intelligence components," as defined in the Definitions Section. 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. Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities.

C1.1.2. The functions of DoD intelligence components not specifically addressed herein shall be carried out in accordance with applicable policy and procedure.

C1.1.3. These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. 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 to 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.

C1.1.4. DoD intelligence components shall not request any person or entity to undertake any activity forbidden by Executive Order 12333 (reference (a)).

C1.2. 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 U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C1.3. INTERPRETATION

C1.3.1. These procedures shall be interpreted in accordance with their stated purpose.

C1.3.2. All defined terms appear in the Definitions Section. Additional terms, not otherwise defined, are explained in the text of each procedure, as appropriate.

C1.3.3. All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned. Questions that cannot be resolved in this manner 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.

C1.4. 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 exception.

C1.5. AMENDMENT

Requests for amendment of these procedures shall be made 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 amendment.

APPENDIX 4: MILITARY SUPPORT
TO LAW ENFORCEMENT

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C2. CHAPTER 2

PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

C2.1. APPLICABILITY AND SCOPE

This procedure 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.

C2.2. EXPLANATION OF UNDEFINED TERMS

C2.2.1. 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. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure 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.

C2.2.2. Cooperating sources means persons 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. These include Government Agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments.

C2.2.3. 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.

C2.2.4. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C2.3. 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:

C2.3.1. Information Obtained With Consent. Information may be collected about a United States person who consents to such collection.

C2.3.2. Publicly Available Information. Information may be collected about a United States person if it is publicly available.

C2.3.3. Foreign Intelligence. Subject to the special limitation contained in section C2.5., below, information may be collected about a United States person if the information constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are:

C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;

C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;

C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;

C2.3.3.4. Persons who are reasonably believed to be prisoners of war; missing in action; or are the targets, the hostages, or victims of international terrorist organizations; or

C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

C2.3.4. Counterintelligence. Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:

C2.3.4.1. Persons 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

C2.3.5. Potential Sources of Assistance to Intelligence Activities. Information may be collected about United States persons reasonably believed to be potential sources of intelligence, or potential sources of assistance to intelligence activities, for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

C2.3.6. 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 that 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:

C2.3.6.1. Present and former DoD employees;

C2.3.6.2. Present or former employees of a present or former DoD contractor; and

C2.3.6.3. Applicants for employment at the Department of Defense or at a contractor of the Department of Defense.

C2.3.7. Physical Security. Information may be collected about a 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.

C2.3.8. Personnel Security. Information may be collected about a United States person that arises out of a lawful personnel security investigation.

C2.3.9. Communications Security. Information may be collected about a United States person that arises out of a lawful communications security investigation.

C2.3.10. Narcotics. Information may be collected about a United States person who is reasonably believed to be engaged in international narcotics activities.

C2.3.11. 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

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

organization, including those who are targets, victims, or hostages of international terrorist organizations.

C2.3.12. Overhead Reconnaissance. Information may be collected from overhead reconnaissance not directed at specific United States persons.

C2.3.13. Administrative Purposes. Information may be collected about a United States person that is necessary for administrative purposes.

C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS

C2.4.1. 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. 12333 (reference (a)), and this Regulation, as appropriate.

C2.4.2. Least Intrusive Means. The collection of information about United States persons shall be accomplished by the least intrusive means. In general, this means the following:

C2.4.2.1. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned;

C2.4.2.2. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources;

C2.4.2.3. 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

C2.4.2.4. 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.

C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES

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

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C2.5.1. 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;

C2.5.2. Such foreign intelligence cannot be reasonably obtained by overt means;

C2.5.3. The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI); and

C2.5.4. The use of other than overt means has been approved in writing by the head of the DoD intelligence component concerned, or his single designee, as being consistent with these procedures. A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy).

APPENDIX 4: MILITARY SUPPORT
TO LAW ENFORCEMENT

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C3. CHAPTER 3

PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

C3.1. APPLICABILITY

This procedure governs the kinds of information about United States persons 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 purposes or is required by law to be maintained.

C3.2. EXPLANATION OF UNDEFINED TERMS

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

C3.3. CRITERIA FOR RETENTION

C3.3.1. Retention of Information Collected Under Procedure 2. Information about United States persons may be retained if it was collected pursuant to Procedure 2.

C3.3.2. Retention of Information Acquired Incidentally. Information about United States persons collected incidentally to authorized collection may be retained if:

C3.3.2.1. Such information could have been collected intentionally under Procedure 2;

C3.3.2.2. Such information is necessary to understand or assess foreign intelligence or counterintelligence;

C3.3.2.3. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation; or

C3.3.2.4. Such information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C3.3.3. 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 such information to the appropriate recipients.

C3.3.4. 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.

C3.3.5. Retention of Other Information. Information about United States persons other than that covered by paragraphs C3.3.1. through C3.3.4., above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

C3.4. ACCESS AND RETENTION

C3.4.1. 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.

C3.4.2. 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.

C3.4.3. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C4. CHAPTER 4

PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

C4.1. APPLICABILITY AND SCOPE

This procedure 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.

C4.2. CRITERIA FOR DISSEMINATION

Except as provided in section C4.3., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

C4.2.1. The information was collected or retained or both under Procedures 2 and 3;

C4.2.2. 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:

C4.2.2.1. 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;

C4.2.2.2. A law enforcement entity of Federal, State, or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce;

C4.2.2.3. 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;

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C4.2.2.4. An Agency of the Federal Government authorized to receive such information in the performance of a lawful governmental function; or

C4.2.2.5. A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

C4.3. OTHER DISSEMINATION

Any dissemination that does not conform to the conditions set forth in section C4.2., 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 Defense. Such approval shall be based on determination that the proposed dissemination complies with applicable laws, Executive orders, and regulations.

APPENDIX 4: MILITARY SUPPORT
TO LAW ENFORCEMENT

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5. CHAPTER 5

PROCEDURE 5. ELECTRONIC SURVEILLANCE

C5.1. PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.1.1. Applicability. This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1979 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

C5.1.2. General Rules

C5.1.2.1. 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.

C5.1.2.2. 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.

C5.1.2.3. Electronic Surveillance In Emergency Situations

C5.1.2.3.1. 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).

C5.1.2.3.2. The head of a 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 subparagraph C5.1.2.2., above, provided the appropriate official concerned shall be advised of such requests as soon as possible thereafter.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.2. PART 2: ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.2.1. Applicability. This part of Procedure 5 applies to electronic surveillance, as defined in the Definitions Section, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 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 persons abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

C5.2.2. Explanation of Undefined Terms

C5.2.2.1. 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 persons 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.

C5.2.2.2. 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.

C5.2.3. Procedures. Except as provided in paragraph C5.2.5., 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. Requests for

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

approval will be forwarded to the Attorney General by an official designated in subparagraph C5.2.5.1., below. Each request shall include:

C5.2.3.1. An identification or description of the target.

C5.2.3.2. A statement of the facts supporting a finding that:

C5.2.3.2.1. There is probable cause to believe the target of the electronic surveillance is one of the following:

C5.2.3.2.1.1. 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;

C5.2.3.2.1.2. A person who is an officer or employee of a foreign power;

C5.2.3.2.1.3. 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 paragraph, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C5.2.3.2.1.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C5.2.3.2.1.5. 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.

C5.2.3.2.2. The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence.

C5.2.3.2.3. The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be obtained by other less intrusive collection techniques.

C5.2.3.3. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.2.3.4. A description of the means by which the electronic surveillance will be effected.

C5.2.3.5. 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.

C5.2.3.6. A statement of period of time, not to exceed 90 days, for which the electronic surveillance is required.

C5.2.3.7. 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 of or concerning United States persons other than those targeted, acquired incidental to such surveillance.

C5.2.4. Electronic Surveillance in Emergency Situations. Notwithstanding paragraph C5.2.3., 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:

C5.2.4.1. Officials designated in paragraph C5.2.5., 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:

C5.2.4.1.1. 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;

C5.2.4.1.2. A person's life or physical safety is reasonably believed to be in immediate danger; or

C5.2.4.1.3. The physical security of a defense installation or Government property is reasonably believed to be in immediate danger.

C5.2.4.2. Except for actions taken under subparagraph C5.2.4.1.2., above, any official authorizing such emergency surveillance shall find that one of the criteria contained in subparagraph C5.2.3.2.1., 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.2.4.3. 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.

C5.2.4.4. 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.

C5.2.5. Officials Authorized to Request and Approve Electronic Surveillance Outside the United States

C5.2.5.1. The following officials may request approval of electronic surveillance outside the United States under paragraph C5.2.3., above, and approve emergency surveillance under paragraph C5.2.4., above:

C5.2.5.1.1. The Secretary and Deputy Secretary of Defense.

C5.2.5.1.2. The Secretaries and Under Secretaries of the Military Departments.

C5.2.5.1.3. The Director and Deputy Director of the National Security Agency/Chief, Central Security Service.

C5.2.5.2. Authorization for emergency electronic surveillance under paragraph C5.2.4., may also be granted by:

C5.2.5.2.1. Any general or flag officer at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered, or

C5.2.5.2.2. The Deputy Director for Operations, National Security Agency.

C5.3. PART 3: SIGNALS INTELLIGENCE ACTIVITIES

C5.3.1. Applicability and Scope

C5.3.1.1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection,

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

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.

C5.3.1.2. 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 that 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.

C5.3.2. Explanation of Undefined Terms

C5.3.2.1. 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 or activities conducted by others and related to 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.

C5.3.2.2. 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.

C5.3.2.3. 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 communications security.

C5.3.2.4. United States Person. For purposes of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person:

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.3.2.4.1. 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 gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.

C5.3.2.4.2. 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.

C5.3.2.4.3. 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.

C5.3.2.4.4. An unincorporated association whose headquarters are located outside the United States may be presumed not to 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.

C5.3.2.5. 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.

C5.3.3. Procedures

C5.3.3.1. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.3.3.2. 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.

C5.3.3.2.1. 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 exercises.

C5.3.3.2.2. 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.

C5.3.3.2.3. 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 reviews and critiques of such exercise.

C5.4. PART 4: TECHNICAL SURVEILLANCE COUNTERMEASURES

C5.4.1. 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)).

C5.4.2. 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 this 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.4.3. 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:

C5.4.3.1. 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;

C5.4.3.2. The use of such countermeasures is limited in that necessary to determine the existence and capability of such equipment; and

C5.4.3.3. Access to the content of communications acquired during the use of countermeasures is limited to persons 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 that 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 only for these purposes. If acquired outside the United States, information that indicates a violation of Federal law, including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be 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.

C5.5. PART 5: DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENT

C5.5.1. Applicability This part of Procedure 5 applies to developing, testing, or 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.

C5.5.2. Procedures

C5.5.2.1. Signals Authorized for Use

C5.5.2.1.1. The following may be used without restriction:

C5.5.2.1.1.1. Laboratory-generated signals.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.5.2.1.1.2. Communications signals with the consent of the communicator.

C5.5.2.1.1.3. Communications in the commercial or public service broadcast bands.

C5.5.2.1.1.4. Communications transmitted between terminals located outside of the United States not used by any known United States person.

C5.5.2.1.1.5. Non-communications signals (including telemetry, and radar).

C5.5.2.1.2. 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.

C5.5.2.1.3. Any of the following may be used subject to the restrictions of subparagraph C5.5.2.2., below.

C5.5.2.1.3.1. Communications over official Government communications circuits with consent from an appropriate official of the controlling agency.

C5.5.2.1.3.2. Communications in the citizens and amateur-radio bands.

C5.5.2.1.4. Other signals may be used only when 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 subparagraph C5.5.2.2., 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.

C5.5.2.2. Restrictions. For signals described in subparagraphs C5.5.2.1.3. and C5.5.2.1.4., above, the following restrictions apply:

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.5.2.2.1. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in paragraph C5.5.1., above.

C5.5.2.2.2. No particular United States person shall be targeted intentionally without consent.

C5.5.2.2.3. The content of any communication shall:

C5.5.2.2.3.1. Be retained only when actually needed for the purposes referred to in paragraph C5.5.1., above;

C5.5.2.2.3.2. Be disseminated only to persons conducting the activity; and

C5.5.2.2.3.3. Be destroyed immediately upon completion of the activity.

C5.5.2.2.4. 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 paragraph C5.5.1., 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 paragraph C5.5.1., or collection avoidance purposes. No content of any communication may be retained or used other than as provided in subparagraph C5.5.2.2.3., above.

C5.6. PART 6: TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

C5.6.1. Applicability. This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operation 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 non-intelligence components.

C5.6.2. Procedures

C5.6.2.1. Training Guidance. The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

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.

C5.6.2.2. Training Limitations

C5.6.2.2.1. Except as permitted by paragraph C5.6.2.2.2. and C5.6.2.2.3., below, the use of electronic communications and surveillance equipment for training purposes is permitted, subject to the following limitations:

C5.6.2.2.1.1. To the maximum extent practical, use of such equipment for training purposes shall be directed against communications that are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure.

C5.6.2.2.1.2. The contents of private communications of non-consenting United States persons may not be acquired aurally unless the person is an authorized target of electronic surveillance.

C5.6.2.2.1.3. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

C5.6.2.2.2. Public broadcasts, distress signals, or official U.S. Government communications may be monitored, provided that when Government Agency communications are monitored, the consent of an appropriate official is obtained.

C5.6.2.2.3. Minimal acquisition of information is permitted as required for calibration purposes.

C5.6.2.3. Retention and Dissemination. Information collected during training that involves communications described in subparagraph C5.6.2.2.1.1., 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 subparagraph C5.6.2.2.1.1., 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 limitation does not apply to distress signals.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.7. PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS

C5.7.1. Applicability and Scope This part of Procedure 5 applies to the conduct of vulnerability surveys and hearability surveys by DoD intelligence components.

C5.7.2. Explanation of Undefined Terms

C5.7.2.1. 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 foreign intelligence services.

C5.7.2.2. 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 hearability of reception over time.

C5.7.3. Procedures

C5.7.3.1. 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 of the following limitations:

C5.7.3.1.1. No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee.

C5.7.3.1.2. No transmission may be acquired aurally.

C5.7.3.1.3. No content of any transmission may be acquired by any means.

C5.7.3.1.4. No transmissions may be recorded.

C5.7.3.1.5. No report or log may identify any United States person or entity except 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 included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C5.7.3.2. 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.

C5.7.3.2.1. Collection. When 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.

C5.7.3.2.2. Processing and Storage. Information collected during a hearability survey must be processed and stored as follows:

C5.7.3.2.2.1. The content of communications may not be recorded or included in any report.

C5.7.3.2.2.2. No microwave transmission may be de-multiplexed or demodulated for any purpose.

C5.7.3.2.2.3. 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 transmissions themselves.

C5.7.3.2.3. Dissemination. Reports may be disseminated only within the U.S. Government. Logs may not be disseminated unless required to verify results contained in reports.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C6. CHAPTER 6

PROCEDURE 6. CONCEALED MONITORING

C6.1. APPLICABILITY AND SCOPE

C6.1.1. 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 6.2., below, and no warrant would be required if undertaken for law enforcement purposes.

C6.1.2. Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes 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 within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure.

C6.1.3. 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.

C6.1.4. 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.

C6.2. EXPLANATION OF UNDEFINED TERMS

C6.2.1. 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.

C6.2.2. Monitoring is within the United States if the monitoring device, or the target of the monitoring, is located within the United States.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C6.2.3. Whether concealed monitoring is to occur where the subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office 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.

C6.3. PROCEDURES

C6.3.1. 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:

C6.3.1.1. Within the United States, a DoD intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by the Department of Defense or otherwise in the course of an investigation conducted pursuant to the Agreement Between the Secretary of Defense and the Attorney General (reference (g)).

C6.3.1.2. Outside the United States, such monitoring may be conducted on installations 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.

C6.3.2. Required Determination. Concealed monitoring conducted under paragraph C6.3.1., requires approval by an official designated in paragraph C6.3.3., 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.

C6.3.3. Officials Authorized to Approve Concealed Monitoring. Officials authorized to approve concealed monitoring under this procedure include the Deputy

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

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, U.S. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C7. CHAPTER 7

PROCEDURE 7. PHYSICAL SEARCHES

C7.1. APPLICABILITY

This procedure applies to nonconsensual 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. DoD intelligence components may provide assistance to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12.

C7.2. EXPLANATION OF UNDEFINED TERMS

Physical search means any intrusion upon a person or a person's property or 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.

C7.3. PROCEDURES

C7.3.1. Nonconsensual Physical Searches Within the United States

C7.3.1.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes. The counterintelligence elements of the Military Departments are authorized to conduct nonconsensual physical searches in the United States for counterintelligence purposes of the person or property of active duty military personnel, when authorized by 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 criteria set forth in subparagraph C7.3.1.2., below.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C7.3.1.2. Other Nonconsensual Physical Searches. Except as permitted by section C7.1., above, DoD intelligence components may not conduct nonconsensual physical searches of persons 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 subparagraphs C7.3.2.2.1., through C7.3.2.2.6., below; and be approved by an official designated in subparagraph C7.3.2.2.3., below. A copy of each such request shall be furnished the General Counsel, DoD.

C7.3.2. Nonconsensual Physical Searches Outside the United States

C7.3.2.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes. The counterintelligence elements of the Military Departments may conduct nonconsensual physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes when authorized by 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 criteria set forth in subparagraph C7.3.2.2.2., below.

C7.3.2.2. Other Nonconsensual Physical Searches. DoD intelligence components may conduct other nonconsensual 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 subparagraph C7.3.2.3., below, to the Attorney General and shall include:

C7.3.2.2.1. An identification of the person or description of the property to be searched.

C7.3.2.2.2. A statement of facts supporting a finding that there is probable cause to believe the subject of the search is:

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C7.3.2.2.2.1. 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, activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities;

C7.3.2.2.2.2. A person who is an officer or employee of a foreign power;

C7.3.2.2.2.3. 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 does not justify a nonconsensual physical search without evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;

C7.3.2.2.2.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

C7.3.2.2.2.5. 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.

C7.3.2.2.3. A statement of facts supporting a finding that the search is necessary to obtain significant foreign intelligence or counterintelligence.

C7.3.2.2.4. 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.

C7.3.2.2.5. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search.

C7.3.2.2.6. 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.

C7.3.2.2.7. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C7.3.2.3. Requests for approval of nonconsensual physical searches under subparagraph C7.3.2.2., must be made by:

C7.3.2.3.1. The Secretary or the Deputy Secretary of Defense;

C7.3.2.3.2. The Secretary or the Under Secretary of a Military Department;

C7.3.2.3.3. The Director, National Security Agency; or

C7.3.2.3.4. The Director, Defense Intelligence Agency.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C8. CHAPTER 8

PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

C8.1. 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. 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.

C8.2. EXPLANATION OF UNDEFINED TERMS

C8.2.1. Mail Within United States Postal Channels includes:

C8.2.1.1. Mail while in transit within, among, and between the United States, its territories and possessions (including mail of foreign origin that is passed by a foreign postal administration, to the United States Postal Service for forwarding to a foreign postal 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, NY; and

C8.2.1.2. International mail enroute to an addressee in the United States or its possessions after passage to United States Postal Service from a foreign postal administration or enroute to an addressee abroad before passage to a foreign postal administration. 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.

C8.2.2. To examine mail means to employ a mail cover with respect to such mail.

C8.2.3. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C8.3. PROCEDURES

C8.3.1. Searches of Mail Within United States Postal Channels

C8.3.1.1. Applicable postal regulations do not permit DoD intelligence components to detain or open first-class mail within United States postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service.

C8.3.1.2. DoD intelligence components may request appropriate U.S. postal authorities to inspect, or authorize the inspection, of the contents of second-, third-, or fourth-class mail in United States postal channels, for such purposes, in accordance with applicable postal 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.

C8.3.2. Searches of Mail Outside United States Postal Channels

C8.3.2.1. DoD intelligence components are authorized to open mail to or from a 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 a nonconsensual physical search under subparagraph C7.3.2.2., of Procedure 7.

C8.3.2.2. 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.

C8.3.3. Mail Covers

C8.3.3.1. 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.

C8.3.3.2. 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, in accordance with appropriate law and procedure of the host government, and any Status of Forces Agreement that may be effect.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C9. CHAPTER 9

PROCEDURE 9. PHYSICAL SURVEILLANCE

C9.1. APPLICABILITY

This procedure applies only to the physical surveillance of United States persons by DoD intelligence components for foreign intelligence and counterintelligence purposes. This procedure does not apply to physical surveillance conducted as part of a training exercise when the subjects are participants in the exercise.

C9.2. EXPLANATION OF UNDEFINED TERMS

The term 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 involving electronic surveillance.

C9.3. PROCEDURES

C9.3.1. Criteria for Physical Surveillance In the United States. Within the United States, DoD Intelligence components may conduct nonconsensual physical surveillances for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence component 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 non-intelligence 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.

C9.3.2. Criteria for Physical Surveillance Outside the United States. Outside the United States, DoD Intelligence components may conduct nonconsensual physical surveillance of United States persons in one of the categories identified in paragraph C9.3.1., 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:

C9.3.2.1. 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;

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C9.3.2.2. That physical surveillance of a United States person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot be obtained by other means.

C9.3.3. Required Approvals for Physical Surveillance

C9.3.3.1. Persons Within DoD Investigative Jurisdiction. Physical surveillances within the United States or that 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.

C9.3.3.2. Persons Outside DoD Investigative Jurisdiction. Outside the United States, physical surveillances 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. Such requests shall indicate coordination with the Central Intelligence Agency.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C10. CHAPTER 10

PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

C10.1. 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.

C10.2. EXPLANATION OF UNDEFINED TERMS

C10.2.1. 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.

C10.2.2. 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.

C10.2.3. 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 persons. Thus, a branch, subsidiary, or office of an organization within the United States, which is physically located outside the United States, is not considered as an organization within the United States.

C10.2.4. Participation refers to any 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 meetings or social gatherings that involve organization members, but are not functions or activities of the organization itself does not constitute participation.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C10.2.5. Participation is on behalf of an agency within the intelligence community when an employee is tasked 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 contacts, or establishing and maintaining cover. If a cooperating source furnishes information to an intelligence agency that he or she obtained by participation within an organization, but was not given prior direction or tasking by the intelligence agency to collect such information, then such participation was not on behalf of such agency.

C10.2.6. Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit.

C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION

Except as permitted herein, employees of DoD intelligence components may participate 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 C10.4., below. Participation without such disclosure is permitted only if it is consistent with the limitations set forth in paragraph C10.3.1., below, and has been approved in accordance with paragraph C10.3.2., below.

C10.3.1. Limitations On Undisclosed Participation

C10.3.1.1. 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.

C10.3.1.2. Limitations On Use of Undisclosed Participation for Foreign Intelligence Purposes Within the United States. Undisclosed participation may not 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 United States persons as potential sources of assistance 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C10.3.1.3. Duration of Participation. Authorization to participate under subparagraphs C10.3.2.1., and C10.3.2.2., shall be limited to the period covered by such participation, which shall be no longer than 12 months. Participation that lasts longer than 12 months shall be re-approved by the appropriate official on an annual basis in accordance with this procedure.

C10.3.1.4. 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.

C10.3.2. Required Approvals

C10.3.2.1. Undisclosed Participation That May Be Approved Within the DoD Intelligence Component. Undisclosed participation on behalf of a DoD intelligence component may be authorized with such component under the following circumstances:

C10.3.2.1.1. 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.

C10.3.2.1.2. Participation in organizations that permit other persons acknowledged to the organization to be employees of the U.S. Government to participate.

C10.3.2.1.3. Participation in educational or professional organizations for the purpose of enhancing the professional skills, knowledge, or capabilities of employees.

C10.3.2.1.4. 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

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

when the sponsoring organization does not require disclosure of the participants' 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.

C10.3.2.2. Participation That May Be Approved By Senior Intelligence Officials. Undisclosed participation may be authorized by the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Assistant Chief of Staff for Intelligence, Department of 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 Investigative Service; the Commanding Officer, Air Force Office of Special Investigations; or their single designees, for the following purposes:

C10.3.2.2.1. 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.

C10.3.2.2.2. For counterintelligence purposes, at the written request of the Federal Bureau of Investigation.

C10.3.2.2.3. 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.

C10.3.2.2.4. To collect information necessary to identify and assess other than United States persons as potential sources of assistance for foreign intelligence and counterintelligence activities.

C10.3.2.2.5. To collect information necessary to identify United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

C10.3.2.2.6. To develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities.

C10.3.2.2.7. Outside the United States, to assess United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C10.4. DISCLOSURE REQUIREMENT

C10.4.1. 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, or the records of the organization concerned.

C10.4.2. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C11. CHAPTER 11

PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES

C11.1. 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. 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.

C11.2. PROCEDURES

C11.2.1. 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.

C11.2.2. 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:

C11.2.2.1. 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

C11.2.2.2. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C11.3. EFFECT OF NONCOMPLIANCE

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

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C12. CHAPTER 12

PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES

C12.1. APPLICABILITY

This procedure applies to the provision of assistance by DoD intelligence components to law enforcement authorities. It incorporates the specific limitations on such assistance contained in E.O. 12333 (reference (a)), together with the general limitations and approval requirements of DoD Directive 5525.5 (reference (i)).

C12.2. PROCEDURES

C12.2.1. Cooperation with Law Enforcement Authorities. Consistent with the limitations contained in DoD Directive 5525.5 (reference (i)), and paragraph C12.2.2., below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:

C12.2.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

C12.2.1.2. Protecting DoD employees, information, property, and facilities;
and

C12.2.1.3. Preventing, detecting, or investigating other violations of law.

C12.2.2. Types of Permissible Assistance. DoD intelligence components may provide the following types of assistance to law enforcement authorities:

C12.2.2.1. 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. 12333 (reference (a));

C12.2.2.2. Incidentally acquired information reasonably 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;

C12.2.2.3. Specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to, Enclosure 3 of DoD Directive 5525.5 (reference (i)); and

C12.2.2.4. 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.

C12.2.2.5. Assistance 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C13. CHAPTER 13

PROCEDURE 13. EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

C13.1. 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.

C13.2. EXPLANATION OF UNDEFINED TERMS

C13.2.1. 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.

C13.2.2. 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 the existence of a contractual relationship.

C13.2.3. Human subjects in this context includes any person whether or not such person is a United States person.

C13.3. PROCEDURES

C13.3.1. 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, in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C13.3.2. 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C14. CHAPTER 14

PROCEDURE 14. EMPLOYEE CONDUCT

C14.1. 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.

C14.2. PROCEDURES

C14.2.1. 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 component by law; Executive order, including E.O. 12333 (reference (a)), and applicable DoD Directives.

C14.2.2. Familiarity With Restrictions

C14.2.2.1. Each DoD intelligence component shall familiarize its personnel with the provisions of E.O. 12333 (reference (a)), this Regulation, and any instructions implementing this Regulation that apply to the operations and activities of such component. At a minimum, such familiarization shall contain:

C14.2.2.1.1. Applicable portions of Procedures 1 through 4;

C14.2.2.1.2. A summary of other procedures that pertain to collection techniques that are, or may be, employed by the DoD intelligence component concerned; and

C14.2.2.1.3. A statement of individual employee reporting responsibility under Procedure 15.

C14.2.2.2. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IQ)) and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect that will achieve the objectives set forth in subparagraph C14.2.2.1., above.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C14.2.3. Responsibilities of the Heads of DoD Components. The Heads of DoD Components that constitute, or contain, DoD intelligence components shall:

C14.2.3.1. Ensure that all proposals for intelligence activities that 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.

C14.2.3.2. Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15.

C14.2.3.3. Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder.

C14.2.3.4. 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.

C14.2.3.5. Ensure that the General Counsel and Inspector General with responsibility for the component, as well as the General Counsel, DoD, and the ATSD(IO), have access to all information concerning the intelligence activities of that component necessary to perform their oversight responsibilities.

C14.2.3.6. Ensure that employees cooperate fully with the Intelligence Oversight Board and its representatives.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C15. CHAPTER 15

PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUESTIONABLE ACTIVITIES

C15.1. APPLICABILITY

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

C15.2. EXPLANATION OF UNDEFINED TERMS

C15.2.1. 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.

C15.2.2. 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).

C15.3. PROCEDURES

C15.3.1. Identification

C15.3.1.1. Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO).

C15.3.1.2. 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 paragraph C15.3.2., 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.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C15.3.1.3. Inspectors General, as part of their oversight responsibilities, shall, as appropriate, ascertain whether any organizations, staffs, or offices within their respective jurisdictions, 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 the activities of such components are in compliance with this Regulation and applicable DoD policy.

C15.3.1.4. 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.

C15.3.2. Investigation

C15.3.2.1. 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.

C15.3.2.2. When appropriate, questionable activities reported to a General Counsel shall be referred to the corresponding Inspector General for investigation, and if reported to an 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.

C15.3.2.3. Investigations shall be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from within the component concerned, or from other DoD Components, when necessary, to complete such investigations in a timely manner.

C15.3.2.4. To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation.

C15.3.3. Reports

C15.3.3.1. Each General Counsel and Inspector General shall report immediately to the General Counsel, DoD, and the ATSD(IO) questionable activities of a serious nature.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoD 5240.1-R, December 1982

C15.3.3.2. Each General Counsel and Inspector General shall submit to the ATSD(IO) a quarterly report describing 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)).

C15.3.3.3. All reports made pursuant to subparagraphs C15.3.3.1., and C15.3.3.2., 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)).

C15.3.3.4. The General Counsel, DoD, and the ATSD(IO) may review the findings of other General Counsels and Inspectors General with respect to questionable activities.

C15.3.3.5. 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.

C15.3.3.6. These reporting requirements are exempt from format approval and licensing in accordance with paragraph VII.G. of Enclosure 3 to DoD Directive 5000.19 (reference (k)).

APPENDIX 4: MILITARY SUPPORT
TO LAW ENFORCEMENT

**Appendix 4-5: DODD 5240.1 - Activities of DOD Intelligence Components
that Affect U.S. Persons**

See next page.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT



Department of Defense DIRECTIVE

NUMBER 5240.01
August 27, 2007

USD(I)

SUBJECT: DoD Intelligence Activities

- References:
- (a) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988 (hereby canceled)
 - (b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence," November 23, 2005
 - (c) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended by Executive Order 13284, January 23, 2003, and Executive Order 13355, August 27, 2004
 - (d) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
 - (e) through (k), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues Reference (a) and implements References (b), (c), and (d); section 188 of Public Law 108-458 (Reference (e)); Executive Order 12863 (Reference (f)); and chapter 36 of title 50, United States Code (Reference (g)).

1.2. Updates policy and provides direction for DoD intelligence activities.

1.3. Shall be the primary authority used as guidance by the Defense Intelligence Components and those performing an intelligence or counterintelligence (CI) function to collect, process, retain, or disseminate information concerning U.S. persons.

1.4. Continues to authorize the publication of DoD 5240.1-R (Reference (h)).

2. APPLICABILITY AND SCOPE

This Directive:

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

DoDD 5240.01, August 27, 2007

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Applies to all intelligence activities conducted by the DoD Components.

2.3. Does not apply to authorized law enforcement activities carried out by the Defense Intelligence Components, or to individuals executing law enforcement missions while assigned to the Defense Intelligence Components.

3. DEFINITIONS

Terms used in this Directive are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. All DoD intelligence and CI activities shall be carried out pursuant to the authorities and restrictions of the U.S. Constitution, applicable law, Reference (c), the policies and procedures authorized herein, and other relevant DoD policies authorized by Reference (b). Special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. persons.

4.2. DoD intelligence and CI activities shall conform to U.S. law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).

4.3. Defense Intelligence and CI shall be the all-source information collection, analysis, sharing, and dissemination capability derived from intelligence and CI activities, operations, and campaign plans, provided to national and defense decision makers and warfighters for military planning and operations.

4.4. Defense Intelligence shall provide accurate and timely warning of threats and of foreign capabilities and intent to national and defense decision makers to allow for consideration of the widest range of options. While Defense Intelligence must be timely, it also must be substantive, thorough, contextual, and useful in form and format.

4.5. Consistent with the need to protect intelligence sources and methods and the provisions of Director of Central Intelligence Directive 8/1 (Reference (i)), the Defense Intelligence and CI Components have an affirmative responsibility to share collected and stored information, data, and resulting analysis with other Defense Intelligence and CI Components, the national Intelligence Community (IC), other relevant Federal agencies, and civilian law enforcement officials, as appropriate. This also applies to the exchange and sharing of terrorism-related

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

information pursuant to Reference (d). Information sharing shall adhere to the requirements and restrictions imposed by Federal law, Executive order, and DoD and DNI policies.

4.5.1. The Defense Intelligence and CI Components shall share collected or stored information in a manner consistent with both the need to protect sources and methods and the need to enable the Defense Intelligence and DoD Components, other Government agencies, and the Intelligence Community, as appropriate, to accomplish their missions and responsibilities.

4.5.2. The broadest possible sharing of intelligence with coalition and approved partner countries shall be accomplished unless otherwise precluded from release by law, explicit direction, or policy.

4.5.3. Original classifiers shall draft intelligence products with a presumption of release and in such a manner as to allow the widest dissemination to allies, coalitions, and international organizations.

4.6. No Defense Intelligence or CI Component shall request any person or entity to undertake unauthorized activities on behalf of the Defense Intelligence or CI Component. No Defense Intelligence or CI Component shall request any person or entity to undertake intelligence activities on behalf of the Defense Intelligence or CI Component that do not follow the procedures described in Reference (h). The collection techniques described in Reference (h) shall be employed only to perform intelligence or CI functions assigned to the Defense Intelligence Component concerned. Use of such techniques to collect information about U.S. persons shall be limited to the least intrusive means feasible and shall not violate law, Executive order, Presidential guidance, or DoD or DNI policy.

4.7. The Defense Intelligence and CI Components and their employees shall report all intelligence or CI activities that may violate law, Executive order, Presidential directive, or applicable DoD policy through the Component chain of command to the Inspector General or General Counsel responsible for the Defense Intelligence Component concerned, or to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)).

4.8. The Defense Intelligence Components shall only conduct, or provide support for the conduct of, covert activities in times of war declared by Congress, during a period covered by a report from the President to Congress consistent with sections 1541-1548 of Reference (g), or when such actions have been approved by the President and directed by the Secretary of Defense.

4.9. Under no circumstances shall any DoD Component or DoD employee engage in, or conspire to engage in, assassination.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)), according to Reference (b), shall provide overall policy guidance for the conduct of DoD intelligence, CI, security, and intelligence-related activities. Pursuant to Reference (b), the USD(I) shall:

5.1.1. Serve as the focal point for the Secretary of Defense, according to the responsibilities and functions prescribed herein, with other U.S. Government entities and agencies, including the National Security Council, the DNI, the Homeland Security Council, the Department of the Treasury, the Department of State, the Department of Justice, and the Department of Homeland Security as well as State agencies, the IC, and Congress.

5.1.2. Serve as the focal point for the Secretary of Defense, according to the responsibilities and functions prescribed herein, with foreign governments, international organizations, and non-governmental organizations.

5.1.3. Promote coordination, cooperation, information sharing, and cross-Service management of intelligence, CI, security, and related programs within the Department of Defense and between the Department and other Federal agencies.

5.1.4. Provide oversight and policy guidance on sensitive intelligence activities; serve as the DoD lead for Departmental participation in all such activities.

5.2. The Department of Defense General Counsel shall:

5.2.1. Serve as the focal point for contact with, and reporting to, the Attorney General regarding legal matters arising under this Directive.

5.2.2. Interpret this Directive and Reference (h), as required.

5.3. The ATSD(IO) shall serve as the focal point for all contacts with the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board pursuant to Reference (f), and shall perform the responsibilities assigned in DoD Directive 5148.11 (Reference (j)).

5.4. The Secretaries of the Military Departments with IC elements shall:

5.4.1. Organize, staff, train, and equip the intelligence assets of the Military Departments, including CI, signals intelligence, geospatial intelligence, measurement and signatures intelligence, and human intelligence assets, to support operational forces, national-level policy-makers, and the acquisition community.

5.4.2. Develop intelligence capabilities including interoperable and compatible systems, databases, and procedures for joint operational forces according to DoD guidance; Combatant Commander and Director, Defense Intelligence Agency, requirements; the Defense Intelligence Information System Network-Centric Architecture; and the Joint Technical Architecture.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

5.4.3. Fulfill assigned Defense Intelligence Analysis Program responsibilities, both national-level and Military Department-unique, for national intelligence activities in support of national and DoD entities through timely, tailored, all-source intelligence tasking, collection, processing/exploitation, analysis/production, and dissemination/integration.

6. EFFECTIVE DATE

This Directive is effective immediately.



Gordon England

Enclosures – 2

- E1. References, continued
- E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Section 188 of Public Law 108-458, “Intelligence Reform and Terrorism Prevention Act of 2004,” December 17, 2004
- (f) Executive Order 12863, “President’s Foreign Intelligence Advisory Board,” September 13, 1993, as amended by Executive Order 13070, December 15, 1997; Executive Order 13301, May 14, 2003; and Executive Order 13376, April 13, 2005
- (g) Chapter 36 and sections 401a(2), 413, and 1541-1548 of title 50, United State Code
- (h) DoD 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,” December 11, 1982
- (i) Director of Central Intelligence Directive 8/1, “Intelligence Community Policy on Intelligence Information Sharing,” June 4, 2004
- (j) DoD Directive 5148.11, “Assistant to the Secretary of Defense (Intelligence Oversight),” May 21, 2004
- (k) Joint Publication 1-02, “DoD Dictionary of Military and Associated Terms,” as amended

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

E2. ENCLOSURE 2

DEFINITIONS

- E2.1. All-Source Analysis. An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement and signature intelligence, and open source intelligence.
- E2.2. CI. Defined in Joint Publication 1-02 (Reference (k)).
- E2.3. Defense CI Components. Defined in Reference (b).
- E2.4. Defense Intelligence. Defined in Reference (b).
- E2.5. Defense Intelligence Components. Defined in Reference (b).
- E2.6. Foreign Intelligence. Defined in section 401a(2) of Reference (g).
- E2.7. Intelligence Activities. The collection, analysis, production, and dissemination of foreign intelligence and CI pursuant to References (b) and (c).
- E2.8. National Intelligence. Defined in Reference (b).
- E2.9. Covert Action. Defined in section 413 of Reference (g).
- E2.10. U.S. Person. Defined in Reference (c).

Appendix 4-6: SECNAVINST 5820.7C - Cooperation with Civilian Law Enforcement Officials

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

SECNAVINST 5820.7C
N3/N5
26 January 2006

SECNAV INSTRUCTION 5820.7C

From: Secretary of the Navy

Subj: COOPERATION WITH CIVILIAN LAW ENFORCEMENT OFFICIALS

Ref: (a) DOD Directive 5525.5 of 15 Jan 86
(b) DOD Directive 3025.12 of 4 Feb 94
(c) Title 10, U.S. Code, Sections 371-382
(d) SECNAVINST 5211.5D
(e) DOD 4515.13-R, Air Transportation Eligibility, of Nov 94
(f) SECNAVINST 5430.107
(g) SECNAVINST 3820.3E
(h) Title 18, U.S. Code, Section 1385
(i) CJCSI 3121.01B

1. Purpose. This instruction implements reference (a) and Department of the Navy (DON) policy, responsibilities, and procedures for the transfer of relevant information, and the provision of equipment, facilities and personnel to Federal, State, and local civilian law enforcement officials. This instruction has been administratively revised and should be reviewed in its entirety.

2. Cancellation. SECNAVINST 5820.7B.

3. Scope. This instruction applies to all DON commands and activities. This instruction does not apply to cooperation with foreign officials (which follows the guidance of applicable international agreements and the administrative and operational chain of command). Use of DON personnel in civil disturbances and related matters is addressed by reference (b). Assistance to the government of the District of Columbia is addressed by separate Department of Defense (DOD) guidance.

4. Policy. It is DON policy to cooperate with civilian law enforcement officials (employees with the responsibility for enforcement of the laws within the jurisdiction of U.S. Federal, State, or local governmental agency) to the extent practical. The implementation of this policy shall be consistent with the needs of national security and military preparedness, the historic tradition of limiting direct military involvement in

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

civilian law enforcement activities, and applicable law. Assistance provided under this instruction shall be at the lowest cost practicable. Assistance may not be provided under this instruction if such assistance could adversely affect national security or military preparedness.

5. Procedures for Prompt Transfer of Relevant Information

a. In accordance with reference (c), DON commands and activities are encouraged to provide Federal, State, or local civilian law enforcement officials any information collected during the normal course of military operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials. In the event that a system of records maintained by DON to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature arising by general statute (or by rule, regulation, or order issued pursuant to the statute), the relevant records in the system of records may be referred, as a routine use under reference (d), to the appropriate agency, whether Federal, State, or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute (or rule, regulation, or order issued pursuant to it). An exception may be made when information is acquired and disseminated to a civilian agency through separate channels established and approved by the Chief of Naval Operations, the Commandant of the Marine Corps, Director, Naval Criminal Investigative Service, or higher authority.

b. The planning, scheduling, and execution of compatible military training or operations may take into account the needs of civilian law enforcement officials when the collection of information is an incidental aspect of training performed for a military purpose. This does not permit the planning, scheduling or execution of military training or operations for the primary purpose of aiding civilian law enforcement officials, or the purpose of routinely collecting information about U.S. citizens. Local law enforcement agents may accompany routinely scheduled training flights as observers for the purpose of collecting law enforcement information. This provision does not authorize the use of DOD aircraft to provide point-to-point transportation and training flights for civilian law enforcement officials (which may be provided only in accordance with reference (e)).

c. The transfer of such information shall be in accordance with reference (f) (providing Naval Criminal Investigative

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

Service exclusive authority for some matters, and primary authority for other matters). Naval commands are authorized to established local contact points with civilian agencies in routine law enforcement matters; commands shall coordinate with the local Naval Criminal Investigative Service Office for other matters.

d. Nothing in this section modifies DON policies or procedures concerning collection or dissemination of information for intelligence purposes under reference (g).

6. Procedures for Request for Equipment, Facilities, Personnel

a. All requests from civilian law enforcement officials for the use of DON equipment, facilities, or personnel under this instruction will be submitted by the requested command via the chain of command to the designated approval authority (unless approval by higher authority is required by statute or DOD guidance). On Marine Corps installations with Provost Marshals, requests shall be coordinated with the Provost Marshal. Requests requiring DoD approval must be forwarded with a recommendation and justification to approve or deny the request. Requests may be communicated by telephone when time and circumstances require immediate action. When forwarding a request, the command will provide all available relevant information concerning:

(1) The ability to provide the assistance requested without adversely affecting national security or military preparedness, and

(2) The incremental costs DON would incur in providing the requested assistance.

b. Approval Authority for Use of Equipment and Facilities:

(1) Requests for the loan or use of equipment or facilities for more than 60 days (including a permanent disposition) or for arms, ammunition, combat vehicles, vessels, and aircraft must be approved by the Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN (M&RA)).

(2) All other requests may be approved by any of the following commands (or superiors to these commands): Naval Component and Fleet Commanders; Commanders and Commanding Officers of major Navy shore commands; Commanding Generals of Marine Corps operating forces; Commanders of Marine Corps bases, camps, aviation installations, logistics installations, and unit

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

training centers; Commanding Generals of Marine Corps Reserve support activities.

c. Approval Authority for Use of Personnel:

(1) The Secretary of Defense, via the Joint Staff (and Assistant Secretary of Defense (Reserve Affairs) for requests involving reserve personnel), is the approval authority for personnel requests that involve assignment of 50 or more DON personnel, or a period of assignment of more than 30 days, or DON intelligence components.

(2) The ASN (M&RA) may approve requests for the following use of DON personnel, except as provided above, in accordance with reference (a):

(a) To provide training or expert advice;

(b) For equipment maintenance;

(c) To monitor and communicate the movement of air and sea traffic;

(3) The Under Secretary of Defense for Personnel and Readiness, via the Joint Staff (and ASD(RA)) for requests involving reserve personnel) is the approval authority for other requests that involve the assignment of personnel.

d. Delegated Denial Authority: Requests for assistance from civilian law enforcement officials that may be approved at the Secretary of the Navy level or below may be denied by the appropriate Echelon 2 command if appropriate under this instruction.

7. Permissible Forms of Equipment and Facilities Assistance

a. DON activities may make equipment and facilities (base and research) available to Federal, State, or local civilian law enforcement officials for law enforcement purposes when approved as above.

b. Approval authorities shall ensure that assistance provided under this paragraph follows applicable provisions of Title 10, U.S. Code, Sections 372, 2576, 2667, Title 31, U.S. Code, Sections 1535-1536, and other applicable laws and directives (see reference (a)).

8. Permissible and Impermissible Forms of Personnel Assistance

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

a. DoD policy (reference (a), making the Posse Comitatus Act applicable to the DON) reflects the historic tradition of limiting direct military involvement in civilian law enforcement activities. The Posse Comitatus Act (reference (h)) states:

"Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."

Pursuant to reference (a), commands must adhere to this paragraph in deciding on the provision of military personnel to civilian law enforcements requests.

b. Restrictions on Direct Assistance: Except as otherwise provided in this instruction, reference (a) prohibits the following forms of direct assistance by military personnel:

(1) Interdiction of a vehicle, vessel, aircraft, or other similar activity.

(2) A search or seizure.

(3) An arrest, apprehension, stop and frisk, or similar activity.

(4) Use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.

(5) With regard to such actions described above that are conducted outside the territorial jurisdiction of the United States, the Secretary of Defense or the Deputy Secretary of Defense will consider for approval, on a case-by-case basis, requests for exceptions to the policy restrictions against direct assistance by military personnel to execute the laws. Such requests for exceptions to policy outside the territorial jurisdiction of the United States should be made only when there are compelling and extraordinary circumstances to justify them.

(6) Further, the Secretary of the Navy may provide exceptions to the limitations contained in this instruction on a case-by-case basis:

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

(a) Such exceptions shall include requests from the Attorney General for assistance under Title 21, U.S. Code, Section 873(b).

(b) Prior approval from the Secretary of Defense shall be obtained for exceptions that are likely to involve participation by members of the Navy or Marine Corps in an interdiction of a vessel or aircraft, a law enforcement search or seizure, an arrest, apprehension, or other activity that is likely to subject civilians to use of military power that is regulatory, proscriptive, or compulsory. Such approval may be granted only when the head of the civilian agency concerned verifies that:

1. The size or scope of the suspected criminal activity poses a serious threat to the interests of the United States and enforcement of a law within the jurisdiction of the civilian agency would be impaired seriously if the assistance were not provided because civilian assets are not available to perform the missions; or

2. Civilian law enforcement assets are not available to perform the mission and temporary assistance is required on an emergency basis to prevent loss of life or wanton destruction of property.

c. Permissible Direct Assistance. The following activities are permissible:

(1) Primary Purpose Military or Foreign Affairs:
Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities. This provision must be used with caution, and does not include actions taken for the primary purpose of aiding civilian law enforcement officials or otherwise serving as a subterfuge to avoid the restrictions of the instruction. Actions under this provision may include the following, depending on the nature of the DOD interest and the authority governing the specific action in question:

(a) Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ).

(b) Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regardless of whether there is a related civil or criminal proceeding.

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

(c) Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation or facility.

(d) Protection of classified military information or equipment.

(e) Protection of DoD personnel, equipment and official guests.

(f) Such other actions that are undertaken primarily for a military or foreign affairs purpose.

(2) Department of Defense Inspector General (DOD IG): Audits and investigations conducted by, under the direction of, or at the request of the DoD Inspector General. This includes drug investigations conducted by Naval Criminal Investigative Service under DoD IG Criminal Investigations Policy Memorandum Number Five on Criminal Drug Investigative Activities of 1 October 1987.

(3) Preserve Public Order: Actions that are taken under the inherent right of the U.S. Government under the Constitution to ensure the preservation of public order and to carry out governmental operations within its territorial limits, or otherwise in accordance with applicable law, by force, if necessary. This authority is reserved for unusual circumstances, and will be used only under reference (b), which permits use of this power in two circumstances:

(a) The emergency authority authorizes prompt and vigorous Federal action, including use of military forces, to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disasters, or calamities seriously endanger life and property and disrupt normal governmental functions to such an extent that duly constituted local authorities are unable to control the situation.

(b) The emergency authority authorizes Federal action, including the use of military forces, to protect Federal property and Federal Government functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection.

(4) Insurgency: Actions taken pursuant to DOD responsibilities under Title 10, U.S. Code, Sections 331-334 and

APPENDIX 4: MILITARY SUPPORT TO LAW ENFORCEMENT

SECNAVINST 5820.7C
26 January 2006

reference (b), relating to the use of the military forces with respect to insurgency or domestic violence or conspiracy that hinders the execution of State or Federal law in specified circumstances.

(5) Assistance to Executive Officials. Actions taken under express statutory authority to assist officials in executing the laws, subject to applicable limitations. The laws that permit direct military participation in civilian law enforcement, include, but are not limited to, the following:

(a) Protection of national parks and certain other Federal lands. Title 16, U.S. Code, Sections 23, 78 and 593.

(b) Enforcement of the Fishery Conservation and Management Act of 1976. Title 16, U.S. Code, Section 1861(a).

(c) Assistance in the case of crimes against foreign officials, official guests of the United States, and other internationally protected persons. Title 18, U.S. Code, Sections 112 and 1116.

(d) Assistance in the case of crimes against members of Congress. Title 18, U.S. Code, Section 351.

(e) Assistance in the case of crimes involving nuclear materials. Title 18, U.S. Code, Section 831.

(f) Protection of the President, Vice President, and other designated dignitaries. Title 18, U.S. Code, Section 1751 and the Presidential Protection Assistance Act of 1976.

(g) Actions taken in support of the neutrality laws. Title 22, U.S. Code, Sections 408 and 461-462.

(h) Removal of persons unlawfully present on Indian lands. Title 25, U.S. Code, Section 180.

(i) Execution of quarantine and certain health laws. 42 U.S.C. § 97.

(j) Execution of certain warrants relating to enforcement of specified civil rights laws. 42 U.S.C. § 1989.

(k) Removal of unlawful inclosures from public lands. 43 U.S.C. § 1065.