V-1

August 2004
CC-0000-181-95

DEFENSE INTELLIGENCE MANAGEMENT DOCUMENT

INTELLIGENCE LAW HANDBOOK

Defense HUMINT Service

V-1

August 2004
CC-0000-181-95

DEFENSE INTELLIGENCE MANAGEMENT DOCUMENT

INTELLIGENCE LAW HANDBOOK

Defense HUMINT Service

Defense Intelligence Agency
Intelligence Law Handbook

TABLE OF CONTENTS

Chapter 9

LIST OF TABLES

Chapter 1

GENERAL INFORMATION

1-1. PURPOSE.

a. This intelligence law handbook provides in one volume a compendium of unclassified guidance pertaining to legal aspects of the Intelligence Community. It describes the statutes underpinning the Intelligence Community, court rulings related to those statutes, and the various Executive Orders, Department of Defense Directives, Director of Central Intelligence (DCI) Directives, and DIA and military Service regulations and manuals implementing the statutes and directives governing the Intelligence Community. This handbook is modelled after USAINSCOM Pamphlet 27-1, "Intelligence Law Handbook", dated 31 January 1986. It includes updated legal and Executive Branch material current as of the information date cutoff.

b. This document is designed to serve as a handy reference tool for all military and civilian DIA and Defense HUMINT Service (DHS) personnel. It should prove particularly useful to legal advisors, intelligence oversight personnel, personnel overseeing or conducting the full range of HUMINT operational activity, DHS headquarters managers and desk officers, military reserve intelligence personnel, and instructors of DHS personnel. This handbook also serves other Intelligence Community personnel and US government officials who interact with the Intelligence Community and must maintain familiarity with its security and oversight provisions.

c. Use of this handbook by DIA personnel will not substitute for legal review or interpretation of specific operations or circumstances surrounding utilization of intelligence collection techniques or operational activities, or for appropriate coordination procedures for intelligence operations as described in DCI and DoD Directives. Full coordination of all DHS operations will be accomplished

(b)(3):10 USC 424,(b)(3):50 USC 3024(i)

1-2. APPLICABILITY. This intelligence law handbook is applicable to all DIA and DHS personnel and elements.

1-3. REFERENCES. See Appendix A for a list of references.

1-4. POLICIES.

a. It is the policy of DIA and the DHS that all personnel will be familiar with the statutes, Executive Orders, DCI Directives, DoD Directives, and DIA manuals and regulations related to

the conduct of intelligence operations and intelligence oversight. Additionally, all DHS personnel will ensure that operations and/or actions undertaken by them or under their purview comply fully with all rules and regulations and immediately notify appropriate DHS or DIA/GC authorities if violations or possible violations come to their attention.

b. This intelligence law handbook itself does not prescribe policies. It provides the framework under which Intelligence Community policies exist and explains how those policies are implemented by DIA and the DHS and how they apply to DHS personnel, units, operations, and missions and functions.

c. In addition, this handbook is designed to help meet the requirements of DIAM 60-4, "Procedures Governing DIA Intelligence Activities That Affect U.S. Persons," which requires that all DIA employees be made aware of the need for assuring compliance with existing laws, directives and regulations. It also will improve the efficiency and understanding of the employment of various sources and methods by DHS personnel.

1-5. INTERPRETATION. All questions of interpretation regarding this handbook or any of the documents described herein should be referred to the DIA/GC or local military legal office responsible for advising the DHS unit concerned.

1-6. NOTES TO CHAPTERS, APPENDICES AND TABLES. Footnotes for the text of this handbook are found on each corresponding page in the text and in the appendices to which they apply. Notes to tables are found at the end of each table.

Chapter 2

INTRODUCTION

2-1. BACKGROUND. President Reagan, and each of his two predecessors in office, Presidents Carter and Ford, issued Executive Orders to put their mark on the conduct of United States intelligence activities.[1] The Reagan order, E.O. 12333, was signed by the President on 4 December 1981,[2] and was the product of the President's desire to give intelligence officers a clear signal that his administration recognized the value and importance of an effective intelligence program and that it had confidence in the men and women of the various components of the Intelligence Community.

a. E.O. 12333 is implemented within the Department of Defense through DoD 5240.1-R, "Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons."[3] This regulation is implemented in DIA and the DHS by DIA Regulation 60-4, "Procedures Governing DIA Intelligence Activities That Affect U.S. Persons". The Services each have issued regulations implementing DoD Directive 5240.1-R. The Army has issued Army Regulation 381-10, "US Army Intelligence Activities". The Navy has issued SECNAV INSTRUCTION 3820.3D, "Oversight of Intelligence Activities Within the Department of the Navy", which governs both Navy and Marine Corps intelligence activities. The Air Force has issued Air Force Instruction 14-104, "Conduct of Intelligence Activities".

b. AR 381-10 represented the culmination and syntheses of numerous attempts since the late 1960s to provide a single-source reference document for the procedural regulation of Army intelligence activities, and is significantly more restrictive than DoD, DIA, and the other Service regulations. As of 1 October 1995 all Service General Defense Intelligence Program (GDIP) HUMINT activities will became part of the DHS and, by extension, DIA employees subject to DIAR 60-4 rather than the individual Service regulations described above. Non-GDIP Army intelligence personnel,

---

[1]The Carter order, E.O. 12036, 24 January 1978, as amended, entitled United States Intelligence Activities, was revoked by E.O. 12333, Pt. 3.6. The Ford order, E.O. 11905, 18 February 1976, as amended, relating to United States foreign intelligence activities, was superseded by E.O. 12036. Presidents Bush and Clinton have each reaffirmed E.O. 12333.

[2]46 C.F.R. 59941.

[3]DoD regulation 5240.1-R was approved by the Attorney General of the United States on 4 October 1982, and signed by the Secretary of Defense on 7 December 1982. It was reissued by Deputy Secretary of Defense William H. Taft, IV, on 25 April 1988.

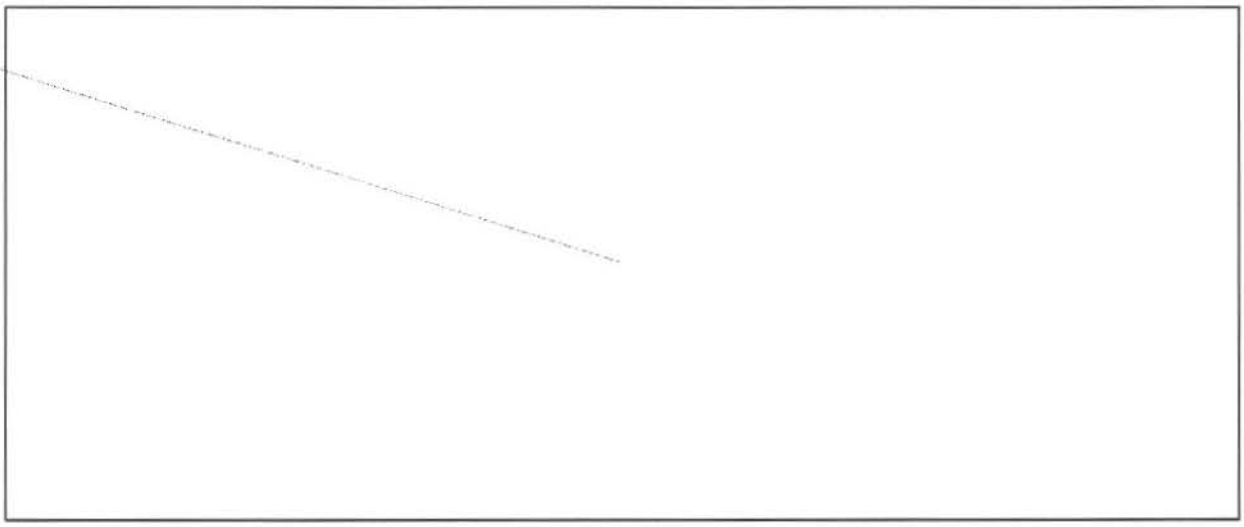
to include tactical HUMINT assets, will continue to fall within the purview of AR 381-10.

c. The material contained in this handbook is intended to familiarize DIA and DHS personnel with some of the more important aspects of E.O. 12333 and DoD 5240.1-R. This material generally follows the format of the DoD regulation, which is divided into 15 separate chapters, called procedures (see table 2-1).

2-2. DOD HUMINT OVERVIEW. A few introductory comments about the consolidation of DIA and Service GDIP HUMINT assets into the DHS and its impact from a legal standpoint are appropriate.

a. On 15 March 1991 the Secretary of Defense approved the Plan for Restructuring Defense Intelligence. This plan was taken a step further for Defense HUMINT with the issuing of DoD Directive 5200.37, "Centralized Management of Department of Defense Human Intelligence (HUMINT) Operations," signed by Deputy Secretary of Defense Donald J. Atwood on 18 December 1992. On 2 November 1993 Deputy Secretary of Defense William J. Perry directed the consolidation of Defense HUMINT into the DHS in accordance with the plan developed by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), in accordance with DoD Directive 5200.37. The purpose of this consolidation was to preserve the Defense Department's ability to manage HUMINT under the constraints of diminishing resources while more rapidly and efficiently focusing the HUMINT elements of the Department on high priority targets worldwide. Emphasis was directed to replace the separate Service and DIA management structures with a single organization, enabling significant cuts in management overhead while preserving field collection capability.

(b)(3):10 USC 424



2-3. CURRENT LATITUDE OF INTELLIGENCE OPERATIONS. In spite of the constraining appearance of all the requirements, under E.O. 12333, DoD Directive 5240.1R, and DIAR 60-4, intelligence activities

conducted by the DHS currently have much more latitude and potential for effectiveness than they have had for quite some time. Timely and accurate information in support of the warfighting CINCs and USG foreign and defense policymakers is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the Unites States receives the best intelligence available.[4]

---

[4]See E.O. 12333, preamble.

Table 2-1
Procedures governing DHS Intelligence activities, DoD 5240.1-R

GENERAL RULE: DoD 5240.1-R applies to all DIA headquarters and field intelligence components; to all DIA personnel when engaged in intelligence activities; and, to members of the National Guard and Reserve when performing duties or engaging in activities directly related to a Federal duty or mission.

PROCEDURES	
Procedure 1	General Provisions
Procedure 2	Collection of Information about United States Persons
Procedure 3	Retention of Information about United States Persons
Procedure 4	Dissemination of Information about United States Persons
Procedure 5	Electronic Surveillance
Procedure 6	Concealed Monitoring
Procedure 7	Physical Searches
Procedure 8	Searches and Examinations of Mail
Procedure 9	Physical Surveillance
Procedure 10	Undisclosed Participation in Organizations
Procedure 11	Contracting for Goods and Services
Procedure 12	Provision of Assistance to Law Enforcement Authorities
Procedure 13	Experimentation on Human Subjects for Intelligence Purposes
Procedure 14	Employee Conduct
Procedure 15	Identifying, Investigating, and Reporting Questionable Activities

Chapter 3

COLLECTION, RETENTION AND DISSEMINATION OF INFORMATION

Section I

Procedure 1 - General Provisions

3-1. GENERAL. DoD 5240.1-R, Procedure 1, is the introductory portion of the regulation. It tells the user what to expect and generally what the regulation covers and what it does not cover. It also sets the tone for the balance of the regulation, a tone which mandates that the activities of "DoD intelligence components,"[5] including the collection of any information by DIA, MUST:

a. Not infringe the constitutional rights of any US person;[6]

b. Be conducted so as to protect the privacy rights of all persons entitled to such protection;[7]

c. Be based on a lawfully assigned function;[8]

d. Employ the least intrusive lawful technique;[9] and

e. Comply with all regulatory requirements.[10]

3-2. SPECIAL ACTIVITIES. "Special Activities" is defined in DoD Directive 5240.1-R as --

---

[5]DoD 5240.1-R, Procedure 1, § A.1. The term "DoD intelligence component" is defined as "All DoD Components conducting intelligence activities, including . . . [t]he National Security Agency/Central Security Service (NSA/CSS)[, and t]he Defense Intelligence Agency (DIA) . . . ." DoD Directive 5240.1-R of April 25, 1988, ¶ C.4.

[6]See DoD 5240.1-R, Procedure 1, § B.

[7]See DoD 5240.1-R, Procedure 1, § B. The specific privacy rights to which a person is entitled depend upon the status of the individual and on the facts and circumstances involved. Those rights run the gamut from full Fourth Amendment constitutional (U.S. Const. amend. IV) protection against unreasonable governmental intrusions, which is generally afforded to all US persons, to virtually no privacy protection for the hostile operative outside the territorial jurisdiction of the United States.

[8]See DoD 5240.1-R, Procedure 1, § B.

[9]The "rule of the least intrusive means" (see infra ¶ 3-16) is limited by E.O. 12333 to "collection of information about techniques . . . within the United States or directed against United States persons abroad." E.O. 12333, Pt. 2.4.

[10]See DoD 5240.1-R, Procedure 1, § A.2.

> Activities conducted in support of national foreign policy objectives abroad, which are planned and executed so that the role of the U.S. Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence U.S. political processes, public opinion, policies, or media, and do not include diplomatic activities or the collection and production of intelligence or related support functions.[11]

a. Only the Central Intelligence Agency is authorized to conduct Special Activities, and it will do so only by express direction of the President. If deemed appropriate by the President, he may direct a specific Special Activity to be conducted by the Department of Defense.[12]

b. Procedure 1 makes it clear that DoD intelligence components are prohibited from conducting or providing support to Special Activities except in time of war, or unless the support has been approved by the Secretary of Defense and the respective Service Secretary.[13]

c. It is important to recognize the distinction between those Special Activities which are characterized under E.O. 12333 and DoD 5240.1-R as "covert and clandestine" activities and the "covert and clandestine" operational activity otherwise carried out routinely in the intelligence community. Note that the definition of "Special Activities" excludes "collections and production of intelligence or related-support functions." Special Activities are only conducted pursuant to a specific Presidential Finding, while the intelligence collection and production is responsive to the intelligence system.

3-3. CONDUCTING SPECIAL ACTIVITIES

a. The meaning of the proscription is not that intelligence components are prohibited from conducting all Special Activities; rather, that such activities must be directed by the President and approved by the Secretary of Defense and the respective Service Secretary. The regulatory flow and tasking structure of the

---

[11]DoD 5240.1-R of April 25, 1988, ¶ C.5.

[12]E.O. 12333, Pt. 1.8(e), states:

> No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution (87 Stat. 855)) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective.

[13]DoD 5240.1-R, Procedure 1, § G.

intelligence community is intended to provide for the flow of such Presidential direction and Secretarial approvals.

b. In sum, unless Special Activities abroad are conducted pursuant to that regulatory and tasking structure, they are prohibited. When tasking and guidance are valid, the Special Activities are, of course, permissible -- within the limits prescribed in the tasking and regulatory control mechanisms.

3-4. PROHIBITION AGAINST ASSASSINATIONS. In addition to the restriction on Special Activities, E.O. 12333, Pt. 2.11, states that "(n)o person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassinations."

3-5. REPORTING POTENTIAL CRIMES.

a. DoD 5240.1-R does not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. When a DoD intelligence investigation or inquiry establishes reasonable belief that a crime has been committed, the DoD intelligence component involved is required to refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 of DoD 5240.1-R (see infra Chapter 8). If the component is otherwise authorized to conduct law enforcement activities, the investigation may be continued under appropriate law enforcement procedures.[14]

b. If evidence surfaces during the course of an investigation by a DoD intelligence component that provides reasonable belief that a crime has been committed, details of the investigation will be provided to the Chief, DIA Office of Security, for action in accordance with DIAR 54-5 and the DIA Inspector General in accordance with DIAM 40-1.

3-6. ADDITIONAL PROVISIONS OF PROCEDURE 1. Additional important features of Procedure 1 are as follows:

a. DoD intelligence components are prohibited from requesting any person or entity to undertake any activity which is forbidden by E.O. 12333 or its implementing directives (e.g., DoD 5240.1-R).[15]

b. Within DIA, requests for exception to policies and procedures established pursuant to E.O. 12333 are to be forwarded

---

[14]DoD 5240.1-R, Procedure 1, § A.3.

[15]DoD 5240.1-R, Procedure 1, § A.4.

through the chain of command to the Secretary of Defense via the DIA General Counsel.[16]

[16]See DIAR 60-4.

Section II

Procedure 2
Collection of Information about United States Persons

3-7. COLLECTION OF INFORMATION.

a. Procedure 2 introduces the reader of DoD 5240.1-R to his or her first entry into the "maze" of the regulation. To begin the journey, it is necessary to stop first and adjust your vocabulary. The terms and words used in DoD 5240.1-R have very specific meanings, and it is often the case that one can be led astray by relying on the generic or commonly understood definition of a particular word. For example, "collection of information" is defined in the Dictionary of the United States Army Terms (AR 310-25) as: "The process of gathering information for all available sources and agencies." But, for the purposes of DoD 5240.1-R, information is "collected" --

> ...only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties...(and) an employee takes some affirmative action that demonstrates an intent to use or retain the information.[17]

b. So, we see that "collection of information" for DoD 5240.1-R purposes is more than "gathering" - it could be described as "gathering, plus...". For the purposes of DoD 5240.1-R, "collection" is officially gathering or receiving information, plus an affirmative act in the direction of use or retention of that information. For example, information received from a cooperating source (e.g., the FBI) about a terrorist group is not "collected" unless and until that information is included in a report, entered into a data base, or used in some other manner which constitutes an affirmative intent to use or retain that information.[18]

3-8. COLLECTABILITY DETERMINATIONS. Information held or forwarded to a supervisory authority, solely for the purpose of making a determination about its collectability (as described in DoD 5240.1-R, Procedure 1), and which has not been otherwise disseminated, is not "collected."[19] Information may be held for up to 90 days pending such a determination from a higher authority, and if that higher level authority finds it necessary to hold the same

---

[17]DoD 5240.1-R, Procedure 2, § B.1.

[18]In addition, data acquired by electronic means is "collected" only when it is processed into intelligible form. DoD 5240.1-R, Procedure 2, § B.1. What constitutes an intelligible form may be somewhat problematic. See also DoD 5240.1-R, Procedure 5, Pt. 1, § F.4, for rules governing the inadvertent interception of conversations of US persons.

[19]DoD 5240.1-R, Procedure 2, § B.1.

information and seek still higher-level advice, an additional period of 90 days will begin to run from the date of the second request. Only when some additional affirmative action is undertaken in the direction of retention or dissemination will such information be considered "collected."[20]

3-9. UNITED STATES PERSONS

a. Another critical term which must be understood to assure an overall understanding of DoD 5240.1-R is "United States person," or US person. When we think of a person, we usually think of Aunt Harriet or Uncle Harry, or Milo Bloom, or some other natural person. In the context of DoD 5240.1-R, a US person is more -- it is a status which attaches to certain persons and entities. Under DoD 5240.1-R, the term United States persons means --

(1) A United States citizen;

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

(3) An unincorporated association, composed mostly of United States citizens or permanent resident aliens; or

(4) A United States corporation, directed and controlled by United States citizens or permanent resident aliens.[21]

b. A person, then, includes non-natural entities, such as associations and corporations, and a US person includes more than US citizens. Examples of non-US persons include a non-immigrant student attending school in the United States, an unincorporated association of foreign persons (even though located in part or wholly in the United States), and a corporation chartered in a foreign country even if it is a subsidiary of a US corporation or corporation chartered in the United States which is controlled by a foreign government.

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

3-10. PRESUMPTIONS OF STATUS.

---

[20]Temporary retention of such material for up to 90 days is permitted. DoD 5240.1-R, Procedure 3, § C.4. Because collectability determinations may require processing through successive levels of command to secure final determinations, it is reasonable to infer that the 90-day period begins anew as each successive requesting component or office seeks a collectability determination from its next level of command or authority.

[21]DoD 5240.1-R, Appendix A, ¶ 27.

a. A person or organization outside the United States may be presumed not to be a United States person unless specific information to the contrary is obtained by the collecting activity.[22]

b. An alien in the United States may be presumed not to be a United States person unless specific information to the contrary is obtained by the collecting activity.[23]

3-11. PREREQUISITES TO COLLECTION.

a. Now that we know what collection means, and we know the definition of a US person, that leads us to the general rule embodied in Procedure 2. In fact, this general rule is the foundational theme throughout DoD 5240.1-R. Information which identifies a United States person may be collected by a DoD intelligence component only --

(1) If the information is necessary to the conduct of a function assigned to that component, and

(2) Provided the information falls into one of the 13 authorized categories listed in table 3-1.

b. If the information is not essential to the mission of the component and it does not fit into one of those categories, then that information may not be collected. However, you will recall from our discussion in paragraph 3-7 that "collection" means receiving plus an affirmative act to use or retain the information.[24] Therefore, mere receipt of non-essential information does not constitute a violation of DoD 5240.1-R. But, as soon as that information is filed or incorporated into other material, or some other act is taken to use or retain the information, then a violation has occurred.

c. One final point about "collection" -- it is not enough that the information meets some of the tests in several of the authorized categories (see table 3-1), nor is it enough that the information is essential to the mission. To be authorized for "collection," information must fully qualify within one or more of the 13 categories, and it must be essential to the conduct of the component's mission (i.e., one of its functions).

3-12. HANDLING QUESTIONABLE INFORMATION. So, what do you do when you receive information which is not "collectable," or when there is doubt about the collectability of information received?

---

[22]DoD 5240.1-R, ¶ 27b.

[23]DoD 5240.1-R, ¶ 27c.

[24]Supra ¶ 3-7a.

a. First, if you know that collection is not permitted, the proper approach is to decline acceptance or take the appropriate steps to burn the document, erase the data, purge it from the system, etc. If the information pertains to the functions of another government agency, it may be sent to such an agency - without retention - for possible use by that agency.[25]

b. Second, if there is doubt about the collectability of the information, then you must seek a collectability determination. You are authorized to retain the information temporarily in your files for up to 90 days pending the receipt of that determination. No dissemination is permitted, except directly to the collectability determination authority.[26] Each organization should have an office or supervisory authority designated to provide advice and assistance on DoD 5240.1-R matters and to assist in rendering collectability determinations. When necessary, a legal interpretation of collectability may be acquired from the DIA General Counsel.

c. If foreign positive intelligence information is collected and deemed suitable for reporting in IIR format, but contains information which identifies U.S. persons or entities, special procedures must be applied. It is imperative that when an IIR makes reference to a U.S. person or entity, the "INSTR" prosign of the IIR be identified as "U.S. YES". This applies to any IIRs which contain the name of a U.S. person (living or deceased), company or ship (U.S. registered private vessels only), or private corporation. A general reference to, "a U.S. citizen" or a company as, "a U.S. aerospace company" does NOT require a "U.S. YES" marking. Only specific references require "U.S. YES" in the "INSTR" prosign of the IIR.

d. Information may be collected about U.S. persons if it can be categorized within one of the exemptions identified in the following Exemptions Listing.[27] If the information is reported using one of the below exemptions, the prosign "U.S. YES" must be followed by the number which corresponds to the exemption. If a collector reports information about a U.S. person or entity, but is

---

[25]E.O. 12333, Pt. 1.1(d), states:

> To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.

[26]See supra ¶ 3-8.

[27]The Exemptions Listing is derived from DoD 5240.1-R, Procedure 2, Paragraph C, "Types of Information that may be Collected about United States Persons", and its subparagraphs.

unable to cite the applicable numeric exemption use, "U.S. YES 16". This should be the exception rather than the rule since reports citing this exemption require special processing by DIA HQ. Collectors citing "U.S. YES" and the applicable number may make appropriate local and lateral electronic dissemination of their reporting. DIA HQ will review all such reporting and notify originators if corrections need to be made or if the information was not appropriate for collection and exemption.

e. Exemptions Listing:

Number:	Description:
1.	Information obtained with the consent of a U.S. person
2.	Publicly available information
3.	Persons acting for or on behalf of (showing allegiance to), a foreign power (or government)
4.	Organizations owned/controlled by a foreign power (or government)
5.	Persons believed to be involved with international terrorist organizations or activities
6.	MIAs, POWs, KIAs, or targets, victims, or hostages of international terrorists
7.	Corporations & commercial organizations (includes individual employees) believed to have some relationship (i.e. trade agreements, contracts) with foreign organizations or persons
8.	Persons involved in collection of intelligence for a foreign power or international terrorist group or persons in contact with such persons
9.	Persons who are potential sources of intelligence or potential sources of assistance to intelligence activities
10.	Intelligence sources who, as present/former DoD employees, or present/former DoD contract employees, or job applicants to DoD, have or had access to, or possess information, which reveals foreign intelligence sources or methods
11.	Persons who are believed to threaten the security of DoD employees, installations, or official visitors
12.	Information which is the result of a lawful personnel or communications security investigation
13.	Narcotics information when individuals (or ships) are believed to be engaging in international narcotics activity
14.	Information collected in support of protecting the safety of persons thought to be the target, victim, or hostage of international terrorists
15.	Information from overhead reconnaissance not specifically directed at U.S. persons
16.	DIA determination requested (only when 1-15 do not clearly apply)

3-13. RESTRICTIVE COLLECTION APPLICABILITY.

a. It is extremely important to recognize that this concept of "restrictive collection" (i.e., as conveyed in DoD 5240.1-R, Procedure 2) applies to all elements of DoD, and not just to counterintelligence and HUMINT operations. The provisions of E.O. 12333 and DoD 5240.1-R are specifically directed at intelligence "components" and not just to selected activities of those components.[28]

b. Whether you are a supply clerk, a computer programmer, a counterintelligence agent, a secretary, a signal security specialist, or a manual morse intercept operator, so long as you are assigned to or attached to DIA, you must be aware of and comply with the mandates of these regulatory documents.

3-14. OTHER POLICY CONSIDERATIONS. Three final policy points about Procedure 2, and then we will move on to a discussion of Procedure 3.

a. First, nothing in Procedure 2 is to be interpreted as authorizing the collection of any information relating to a United States person solely because of lawful advocacy of measures opposed to Government policy.[29]

b. Second, regardless of where collected, and regardless of the category of information, collection must be accomplished by the least intrusive means possible. For example, where it is possible to acquire essential information in one of the 13 authorized categories from public files, rather than from covert investigation, then the choice of "publicly available information" must be used.

c. Third, within the United States, foreign intelligence information (number 3 on the list of 13 authorized categories) may only be collected by overt means, unless specific approval has been granted in writing by the head of a DoD intelligence component, or his or her single designee, to use other means. The Director, Defense Intelligence Agency, and the Director, Defense HUMINT Service are heads of DoD intelligence components for this purpose.

---

[28]"Restrictive collection", as a concept, is found in DoD 5240.1-R, Procedure 2, § C, and implements the provisions of E.O. 12333, Pt. 2.3, which states:

> Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order.

[29]DoD 5240.1-R, Procedure 2, § A.

The Secretary of Defense has designated the Director, Defense Intelligence Agency as the DoD HUMINT Manager (See DoD 5200.37). The Director, DIA, has delegated management of the DoD HUMINT System to the Director, Defense Humint Service. Information copies of approvals by the Director, Defense Intelligence Agency, or Director, Defense HUMINT Service must be forwarded to Deputy Under Secretary of Defense (Policy), and must reflect coordination with the DIA General Counsel.[30]

---

[30]DoD 5240.1-R, Procedure 2, § E.

Table 3-1
Types of collectable information, DoD 5240.1-R, Procedure 2

GENERAL RULE: Information which identifies a United States person may be collected by a DoD intelligence component only if the information is necessary to a function assigned to that component, and provided it falls into one of the authorized categories of collectable information.

AUTHORIZED CATEGORIES OF COLLECTABLE INFORMATION	
Category 1	Information obtained with consent.
Category 2	Publicly available information.
Category 3	Foreign intelligence information. 1/
Category 4	Counterintelligence information. 2/
Category 5	Information pertaining to potential sources of assistance to intelligence activities. 3/
Category 6	Information concerning the protection of intelligence sources and methods. 4/
Category 7	Physical security information.
Category 8	Personnel security investigative information. 5/
Category 9	Communications security information.
Category 10	Information about persons believed engaged in international narcotics activities.
Category 11	Information needed to protect the safety of a person or organization.
Category 12	Information from overhead reconnaissance not directed at specific US persons.
Category 13	Information that is necessary for administrative purposes.

Table 3-1
Types of collectable information, DoD 5240.1-R, Procedure 2

NOTES:

1/ The intentional collection of foreign intelligence about United States persons is limited to persons who are:

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

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

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

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

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

2/ The intentional collection of counterintelligence about United States persons must be limited to:

a. Persons reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.

b. Persons in contact with persons described above for the purpose of identifying such persons and assessing their relationship with those described above.

3/ Information may be collected by 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 and credibility. This category does not include investigations undertaken for personnel security purposes.

Table 3-1
Types of collectable information, DoD 5240.1-R, Procedure 2

4/ Information may be collected by United States persons who have access to, or had access to, or are otherwise in possession of, information which reveals foreign intelligence and counterintelligence sources or methods, when collection is reasonably believed necessary to protect against unauthorized disclosure of such information; provided that within the United States, intentional collection of such information is limited to persons who are:

a. present and former DoD employees;

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

c. Applicants for employment at DoD or a contractor of DoD.

5/ This category includes information concerning relatives and associates of the subject of the investigation, if required by the scope of the investigation and the information has a bearing on the matter being investigated or the security determination being made.

Section III

Special Collection Techniques

3-15. CONSTRAINTS ON THE USE OF SPECIAL COLLECTION TECHNIQUES.

a. Special collection techniques are those lawful investigative techniques which are employed by a DoD intelligence component under the rule of the least intrusive means, after a determination has been made that the required information is not publicly available, available with the consent of the person or persons concerned, or available from cooperative sources.[31]

b. DoD 5240.1-R, Procedures 5 through 10, cover special collection techniques. These include the following:

(1) Procedure 5 - Electronic Surveillance

(2) Procedure 6 - Concealed Monitoring

(3) Procedure 7 - Physical Searches

(4) Procedure 8 - Searches and Examination of Mail

(5) Procedure 9 - Physical Surveillance

(6) Procedure 10 - Undisclosed Participation in Organizations

3-16. RULE OF THE LEAST INTRUSIVE MEANS.

a. The Least Intrusive Means Rule is found in E.O. 12333, part 2.4, and is implemented in DoD 5240.1-R, Procedure 1, section A.4 and Procedure 2, section D. It simply states that the collection of information by a DoD intelligence component must be accomplished by the least intrusive means or lawful investigative technique reasonably available. This rule prescribes a hierarchy of collection techniques which must be considered before an intelligence component engages in collection of information about US persons. The methodologies below become progressively more intrusive as one proceeds through this hierarchical framework. (Also see table 3-2).

(1) First, to the extent feasible, information must be collected from publicly available materials, or with the consent of the person or persons concerned.

(2) Next, if collection from these sources is not feasible, then cooperating sources may be used.

---

[31]See DoD 5240.1-R, Procedure 1, § A and Procedure 2, § D.

(3) Third, if neither publicly available information nor cooperating sources are sufficient or feasible, then collection may be pursued using other lawful investigative techniques that require neither a judicial warrant nor the approval of the Attorney General of the United States.

(4) Finally, when none of the first three approaches has been sufficient or feasible, then the collecting intelligence component may seek approval for use of one of the techniques that require a warrant or the approval of the Attorney General.

b. In most cases, DoD intelligence special collection techniques will fall into the first three categories in the hierarchical scheme of collection techniques. However, as you will see later, a slight twist in the circumstances could easily turn a proposed collection effort from one that could be approved at a local level into one that requires a court order (i.e., judicial warrant) or approval by the Attorney General.

c. For example, consensual physical searches, which yield a wealth of information, may be conducted by a DoD intelligence component pursuant to any lawful function assigned to that component.[32]

3-17. THE CONVERGENCE OF COLLECTION AND LAW ENFORCEMENT RULES

a. While we are on the subject of employment of these various techniques for law enforcement purposes, it is important to point out a distinction between DoD intelligence use of these more intrusive means of collection, and their use in more traditional law enforcement practices. DoD intelligence use of these techniques is limited by those lawful functions assigned to the component desiring to employ a specific technique in a specific set of circumstances, even when the approval authority for such employment has been substantially decentralized.[33]

b. To illustrate, the authority to approve physical surveillance of non-US persons abroad may be delegated to field supervisors.[34] However, an essential prerequisite to the exercise of that approval authority is that the physical surveillance must be conducted for a lawful function assigned to that component. Thus, although a field supervisor in an overseas counterintelligence unit may approve physical surveillance (assuming delegation in writing has been issued) of a non-US person for any function assigned to that unit, the same field supervisor could not approve

---

[32]DoD 5240.1-R, Procedure 7, § C.1.a.

[33]DoD 5240.1-R, Procedure 1, § A.1.

[34]DoD 5240.1-R, Procedure 9, § C.4.c.

a physical surveillance in support of a criminal investigation, or in furtherance of a commander's inquiry regarding a member of the unit.

3-18. THE NEED FOR CAUTION AND ADVICE.

a. This area of DoD intelligence activities, that is, the use of special collection techniques, is the area in which there tends to be the greatest amount of confusion regarding the limitations on permissible activities. Because of this confusion, this area also tends to be the most fertile ground for both abuse and unnecessarily restrictive interpretation of the rules. To be sure, it is fundamental that abuse of the legitimate DoD intelligence and counterintelligence resources and authority must be avoided. The rights of US persons must also be protected, and no intrusion into these protected areas is permissible without first meeting constitutional standards, and then only through a system of careful scrutiny of the intruding apparatus.

b. Nevertheless, we must be mindful of too much caution. We must remember that we are engaged in a real-world mission that involves unprincipled adversaries, and a plethora of sophisticated technical collection and counter-collection enterprises and devices. Terrorism and espionage have destruction as their common denominator, and we are fueling their malignancy when we unnecessarily restrain or restrict our foreign intelligence or counterintelligence efforts, just the same as we would damage the fiber of our democracy through abusive use of our own capabilities and powers.

c. Our business is one that involves constant vigilance and omnipresent balancing of competing interests. To survive, we must take risks. To succeed, we must minimize those risks. To preserve our precious ideals, we must carefully pursue our crafts in such a manner as to not offer up the rights and dignity of our citizens in exchange for that success. To provide these assurances, it is essential that all operations or portions of operations involving special collection techniques (i.e., concealed monitoring, physical searches, searches and examination of mail, and physical surveillance) be thoroughly scrutinized before they begin. This must always be done within the operational chain of command, and where appropriate, or simply where a disinterested perspective is desired, it should include the supporting staff judge advocate or legal advisor.

3-19. ELEMENTS OF COMMONALITY

a. All special collection techniques have two similar primary elements. First, each has the capability of yielding boundless amounts of information about the targets of our collection or the subjects of our investigations. Second, the use of each is constrained by a system of rules designed to protect the legitimate

interests of those targets and subjects. It is important for us as intelligence professionals to accept these elements as indivisible. If we accept only one without the other, we seal a bargain for either abuse or mission failure.

b. In the first instance, special collection techniques must always remain in our repertoire of prospective tools in our quest for mission perfection. In the second instance, we must never consider the employment of these particular tools without concurrent consideration of the rules of engagement. Whether we view the use of special collection techniques as soldiers who must know and respect the law of war, or as citizens who must know and respect the constitution, the results are the same.

3-20. THE PENDULUM SWINGS. Too often we have unnecessarily restricted our efforts because we either too strictly interpret the rules applicable to special collection techniques, or because we have been deterred, if not confounded, by myriad seemingly endless constraints. Some assert that this is the pendulum affect, a reaction to a previously abusive era. Others more pragmatically suggest that our business, as with all else, is evolutionary where one stage begets the next. Whatever the reason, it is past time for us to be so concerned about why the pendulum is where it is. What is essential is that we in the DoD intelligence business permanently vest in ourselves a capable sophistication to make maximum use of all authorized collection techniques. The rules of engagement by which we must operate are not hindrances - they are keys to success.[35]

[35]See infra chapter 5, § IV.

Table 3-2
Rule of the least intrusive means, DoD 5240.1-R

GENERAL RULE: Information may be gathered by DoD intelligence components by any lawful means, provided all collection is based on proper function, employs the least intrusive lawful investigative technique reasonably available, and complies with the procedures of DoD 5240.1-R. 1/

IF IT IS NOT FEASIBLE OR SUFFICIENT	THEN
1. To collect from publicly available information or with the consent of the person concerned...	...information may be collected from cooperating sources.
2. To collect from cooperating sources...	...information may be collected using other lawful techniques which do not require a judicial warrant or Attorney General approval.
3. To collect using other lawful techniques that do not require a judicial warrant or Attorney General approval...	...approval for the use of investigative techniques that require a judicial warrant or approval by the Attorney General may be sought.2/

NOTES:

1/ The techniques contemplated by this rule are the "special collection techniques" described in and regulated by DoD 5240.1-R, Procedures 5 through 10: electronic surveillance, concealed monitoring, physical searches, searches and examination of mail, physical surveillance, and undisclosed participation in organizations.

2/ Request to engage in collection techniques which require DIA or higher-level approval must be submitted through the chain of command to the Secretary of Defense via the DIA General Counsel. The procedures and standards applicable to those requests are discussed in detail in chapters 4 through 7 of this handbook.

Section IV

Procedure 3
Retention of Information About United States Persons

3-21. RETENTION OF INFORMATION.

a. Once again, we must cautiously examine the vocabulary used in DoD 5240.1-R. The term "retention" means more than merely retaining information in files - it is retention plus retrievability. As stated in DoD 5240.1-R --

> ...the term retention as used in this procedure, refers only to the maintenance of information about United States persons which can be retrieved by reference to the person's name or other identifying data.[36]

b. A very limited view must be taken of this retrievability element. Accordingly, if "nonretainable" information can be retrieved by any means, it must be destroyed. From a policy perspective, it is also important to recognize that information that never should have been collected in the first place must also be destroyed, regardless of whether or not it is retrievable. You may not file unauthorized information about US persons just because it is not retrievable by reference to a person's name or other identifying data. That would not be within the spirit and intent of E.O. 12333 and DoD 5240.1-R, which is to allow collection and retention only when necessary to the performance of a lawful function of the particular intelligence agency involved. The initial lawful function threshold test must always be met. So, if buried somewhere you have "nonretainable" information on Aunt Harriet, Uncle Harry or Milo Bloom, go get it and purge it from the files.[37]

3-22. DELETION OF IDENTIFYING DATA. If necessary, you may delete the names of US persons from some files, and substitute a generic term or symbol, but only when retention of the material is otherwise necessary. The premise from which we must always begin, however, is that we do not retain US person information, even if originally collectable, if it is not necessary to an ongoing mission or function.

---

[36]DoD 5240.1-R, Procedure 3, § B.

[37]Where the retention of information is required for administrative purposes, or where such retention is required by law, the rules and restrictions of Procedure 3 do not apply. DoD 5240.1-R, Procedure 3, § A. See also DoD 5240.1-R, Procedure 3, § D.3, which provides that information acquired prior to 1 December 1982, the effective date of E.O. 12333, may be retained without screening so long as retention was in compliance with applicable law and previous executive orders.

3-23. INCIDENTALLY ACQUIRED INFORMATION. Information about US persons collected incidentally to authorized collection may be retained if it could have been collected intentionally under Procedure 2, or --

a. The information is necessary to understand or assess foreign intelligence or counterintelligence;

b. The information is foreign intelligence or counterintelligence collected from electronic surveillance authorized pursuant to DoD 5240.1-R, Procedure 5; or

c. The information is incidental to authorized collection and may indicate involvement in activities that may violate federal, state, local, or foreign law.[38]

3-24. DURATION OF RETENTION.

a. Disposition of information about US persons retained in files must comply with the disposition schedules approved by the Archivist of the United States for files or records in which the information is retained.[39]

b. Information about US persons in DoD intelligence files must be reviewed periodically. This review must ensure that --

(1) The information's continued retention serves the purpose for which it was collected and stored, and

(2) That it is necessary to the conduct of authorized functions of the DoD intelligence component concerned, or other Government agencies.

c. Periodic reviews must be conducted in conjunction with the annual review of files under DIAR 13-1, as appropriate.

d. See table 3-3 for the general rule and criteria for retention of information about US persons.

---

[38]DoD 5240.1-R, Procedure 3, § C.2.

[39]DoD 5240.1-R, Procedure 3, § D.2.

Table 3-3
Retention of Information about US persons, DoD 5240.1-R, Procedure 3

GENERAL RULE: Information about US persons may not be knowingly retained by DoD intelligence components without the consent of the person whom the information concerns, except solely for administrative purposes, or in accordance with the specific retention criteria of Procedure 3.

CRITERIA FOR RETENTION	
1. Information collected under Procedure 2	Information about US persons may be retained if it was collected pursuant to DoD 5240.1-R, Procedure 2.
2. Information acquired incidentally	Information about US persons collected incidentally to authorized collection may be retained if: a. It could have been collected intentionally under Procedure 2. b. It is necessary to understand or assess foreign intelligence or counterintelligence. c. It is foreign intelligence or counterintelligence collected pursuant to approved electronic surveillance. d. It is incidental to authorized collection and indicates activities that may violate federal, state, local, or foreign law.
3. Information relating to functions of other US Government agencies	Information that pertains solely to functions of other US agencies may be retained only as necessary to convey to the appropriate agencies.
4. Temporary retention	Information about US persons may be held up to 90 days to determine permanent retainability under the retention criteria of DoD 5240.1-R.
5. Other information	Information about US persons not covered above may be held only to report or investigate the oversight.

Section V

Procedure 4
Dissemination of Information About United States Persons

3-26. DISSEMINATION OF INFORMATION.

a. DoD 5240.1-R, Procedure 4, is relatively straightforward. It governs the criteria for dissemination of information about United States persons, without their consent, which a DoD intelligence component has collected and retained about such persons. Obviously, if consent has been given, then dissemination is permitted to the extent of that consent.[40]

b. Procedure 4 does not apply to information collected solely for administrative purposes; or dissemination pursuant to law; or pursuant to a court order that otherwise imposes controls upon such dissemination.[41]

3-27. DISSEMINATION DETERMINATIONS. A dissemination determination under Procedure 4 involves a two-step process.[42]

a. First, the holder of the information must make a determination that the prospective recipient will use the information for a lawful government function, and that the information is needed by that prospective recipient for that particular function.

b. Second, once this threshold test has been met, then the information must be determined to fit into one of five categories before it may be disseminated without the consent of the US person or persons to whom it applies. Those five categories each involve a particular kind of prospective recipient, and a particular purpose in their potential use of the information. The information must fit completely into one of those categories. Table 3-4 displays the five categories and the conditions for dissemination.

3-28. OTHER DISSEMINATION. Any dissemination beyond the permissible limits of Procedure 4 must be approved in advance by the DIA

---

[40]DoD 5240.1-R, Procedure 4, § A.

[41]DoD 5240.1-R, Procedure 4, § A. Where dissemination is required pursuant to law or court order, it must be concluded that the specific law or order takes precedence to and overcomes any impediment to such dissemination otherwise contained in executive orders, or executive branch directives or regulations, unless the constitutionality of such a law or court order is properly challenged in an appropriate judicial forum.

[42]DoD 5240.1-R, Procedure 4, § B.2.

General Counsel, following coordination with the Department of Justice and the General Counsel of the Department of Defense.[43]

3-29. DEFINITION OF DISSEMINATION. Neither E.O. 12333 nor DoD 5240.1-R define dissemination. It seems clear, however, that the dissemination criteria apply only to information collected or retained under both Procedures 2 and 3 of DoD 5240.1-R. It is also clear that the considerations of the Freedom of Information Act (see DIAR 12-39) and the Privacy Act (see DIAR 12-12) override the executive order and the departmental regulations. Releases of information under those statutes requires different kinds of tests and considerations. For DIA, if an issue involving the Freedom of Information or Privacy Acts arises, the matter must be referred to the DIA Freedom of Information and Privacy Office.

[43]DoD 5240.1-R, Procedure 4, § C.

Table 3-4
Dissemination of information about US persons, DoD 5240.1-R, Procedure 4

GENERAL RULE: DoD intelligence components may disseminate information about US persons without the consent of those persons only under the conditions and criteria prescribed in DoD 5240.1-R, Procedure 4.

IF THE PROSPECTIVE RECIPIENT IS	THE INFORMATION TO BE DISSEMINATED
1. An employee of the DoD or a DoD contractor	Must be needed in the course of that employees official duties.
2. A federal, state, or local law enforcement entity	Must indicate involvement in activities which may violate laws that entity is responsible to enforce.
3. An agency within the intelligence community	May be disseminated without prior determination of potential need to allow the prospective recipient agency to determine its relevancy.
4. A non-law enforcement, non-intelligence agency, of the federal government	Must be related to the performance of a lawful governmental function of that agency.
5. A foreign government	Must be authorized for dissemination and undertaken pursuant to an agreement or other understanding with that government.

NOTES:

1. Any dissemination that does not conform to the conditions set forth 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 must be based on a determination that the proposed dissemination complies with applicable laws, executive orders, and regulations. Requests by DIA intelligence components will be forwarded through the chain of command to the Secretary of Defense via the DIA General Counsel.

2. Releases of information under the Freedom of Information and Privacy Acts are governed by DIAR 12-39 and DIAR 12-12, respectively, and within DIA are under the cognizance of the DIA Freedom of Information and Privacy Office.

Chapter 4

PROCEDURE 5 - ELECTRONIC SURVEILLANCE

Section I

Introduction

4-1. SCOPE OF PROCEDURE 5. DoD 5240.1-R, Procedure 5, implements the Foreign Intelligence Surveillance Act,[44] or the "FISA", as it is often called, and applies to the following DoD intelligence activities:

a. All electronic surveillance conducted within the United States to collect "foreign intelligence information," as defined in the FISA;[45]

b. All electronic surveillance conducted by DoD intelligence components against US persons outside the United States for foreign intelligence and counterintelligence purposes;[46]

c. Signals intelligence activities, by elements of the United States Signals Intelligence System, that involve collection, retention, and dissemination of foreign communications and military tactical communications;[47]

---

[44]Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (hereinafter called FISA). Procedure 5 also contains departmental implementation of E.O. 12139, Exercise of Certain Authority Respecting Electronic Surveillance, 23 May 1979 (44F.R. 20311, 50 U.S.C.A. § 1803 note). Under E.O. 12139 the President has authorized the Attorney General of the United States to (i) approve electronic surveillance to acquire foreign intelligence information without a court order after certification as required by FISA § 102(a)(1) [50 U.S.C. § 1802(a)(1)]; and (ii) approve applications to the appropriate court under FISA § 103 (50 U.S.C. § 1803) to obtain electronic surveillance orders for foreign intelligence purposes.

E.O. 12139 further designates various executive branch officials to make certificates required by FISA § 104(a)(7) [50 U.S.C. § 1804(a)(7) in support of applications to conduct electronic surveillance. Those officials include the Secretary and Deputy Secretary of State, Secretary and Deputy Secretary of Defense, and the Director and Deputy Director of Central Intelligence. Delegation of this certification authority is limited to persons acting in the capacity of those officials designated in E.O. 12333 and who have been appointed to their positions by the President with the advice and consent of the Senate. Within the Department of Defense, certification authority has been delegated to the Secretary and Under Secretary of each military department and to the Director, National Security Agency. DoD 5240.1-R, Procedure 5, Pt.1, § B.2.

[45]DoD 5240.1-R, Procedure 5, Pt. 1, § A.

[46]DoD 5240.1-R, Procedure 5, Pt. 2, § A.

[47]DoD 5240.1-R, Procedure 5, Pt. 3.

d. DoD intelligence use of electronic equipment for technical surveillance countermeasures purposes;[48]

e. Developing, testing and calibration, by DoD intelligence components, of electronic equipment, that can be used to intercept or process communications and noncommunications signals;[49]

f. Training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment;[50] and

g. *The conduct of vulnerability and hearability surveys by* DoD intelligence components.[51]

4-2. COMPLEXITY OF PROCEDURE 5. In covering these seven different electronic surveillance areas, and their related matters, Procedure 5 is the most complex of all procedures contained in DoD 5240.1-R. Any person who has specific duties involving any particular aspect of electronic surveillance must be thoroughly familiar with details contained in the applicable portions of Procedure 5; and, in most cases, must also study the additional DoD pertinent implementing instructions.

4-3. LAW ENFORCEMENT ACTIVITIES.

a. Before we begin, it is important that we distinguish the electronic surveillance activities which are addressed in DoD 5240.1-R, Procedure 5, from interception of wire and oral communications for law enforcement purposes. The coverage of Procedure 5 is confined to electronic surveillance activities of DoD intelligence components for foreign intelligence and counterintelligence purposes, and to certain technical aspects of electronic surveillance which are closely allied with foreign intelligence collection and counterintelligence activities.

b. The policies, procedures, and restrictions governing interception of wire and oral communications and the use of pen registers and related devices for law enforcement purposes, both in the United States and abroad, are covered in other DoD publications. DoD 5240.1-R, Procedure 5, does not alter any of those provisions, and does not impede upon a commander's authority or responsibility in the areas enumerated in those publications, or in any other area where a commander is executing his authority and

---

[48]DoD 5240.1-R, Procedure 5, Pt. 4.

[49]DoD 5240.1-R, Procedure 5, Pt. 5.

[50]DoD 5240.1-R, Procedure 5, Pt. 6.

[51]DoD 5240.1-R, Procedure 5, Pt. 7.

responsibility as a commander to maintain discipline within his command.[52]

[52]In certain circumstances, a military judge or commander may approve electronic surveillance for law enforcement purposes pursuant to the Manual for Courts-Martial, 1984, Military Rules of Evidence. The mere fact that a commander may be the commander of an intelligence component does not diminish or otherwise change this law enforcement authority.

Section II

The Foreign Intelligence Surveillance Act

4-4. PURPOSE OF THE FISA.

a. The FISA was designed to clarify and make more explicit the role of the federal government in the use of electronic surveillance to obtain foreign intelligence and counterintelligence information (including information pertaining to international terrorist activities), and to provide safeguards for individuals subjected to such surveillance. The Act represents the first time in our history that clandestine intelligence activities of our government have been subject to the regulation of, and coverage by, the positive authority of public law.

b. The Senate Intelligence Committee's [53] report recommending favorable action on the FISA set forth two objectives for the Act -- to enhance US intelligence capabilities and to protect constitutional rights. The report described the FISA as designed to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights."[54] The Committee expected the FISA...

> ...would allow electronic surveillance in circumstances where, because of uncertainty about the legal requirements, the Government may otherwise be reluctant to use this technique for detecting dangerous foreign intelligence and terrorist activities by foreign powers in this country.[55]

4-5. THE DELICATE BALANCING TASK.

a. Managing the correlation between adequate intelligence to guarantee our nation's security on the one hand, and preservation of basic human rights on the other, is a challenging and extremely delicate balancing task. Nevertheless, that balance is absolutely essential in our society; and, it must be achieved without sacrificing either our nation's security, or the civil liberties of United States citizens and of those non-citizens who are entitled to the protection of the Constitution of the United States. The FISA truly strikes that balance. It provides the mechanism to assure that any abuses of the past will remain in the past, while concurrently permitting sanction for legitimate intelligence activities. In its recent report, "The Foreign Intelligence

---

[53] S. Rep. 701, 95th Cong., 2d Sess. (1978).

[54] S. Rep. 701, 95th Cong., 2d Sess. at 16.

[55] S. Rep. 701, 95th Cong., 2d Sess. at 16.

Surveillance Act of 1978: The First Five Years",[56] the Senate Select Committee on Intelligence stated:

> The Committee has reviewed the five years of experience with FISA and finds that the Act has achieved its principal objectives. Legal uncertainties that had previously inhibited legitimate electronic surveillance were resolved, and the result was enhancement of U.S. intelligence capabilities. At the same time, the Act has contributed directly to the protection of the constitutional rights and privacy interests of U.S. persons.[57]

b. Indeed, now that the FISA has been in effect for nearly two decades, most concerned professionals in the intelligence community agree that the standards articulated in the Act have workably accommodated the need for flexibility in the conduct of legitimate surveillance for foreign intelligence and counterintelligence purposes with the mandate to protect individual rights.

4-6. HOW DOES THE FISA WORK?[58]

a. To understand the Act's impact, it is necessary to know something about the surveillance methods used by the US Government. More than just conventional telephone taps and hidden microphones are involved. The FISA defines four categories of electronic surveillance:

(1) Wiretaps. Unconsented acquisition by a surveillance device of the contents of a wire communication to or from a person in the United States, if the acquisition occurs in the United States. This includes not only voice communications, but also teleprinter, telegraph, facsimile, and digital communications. International communications are covered if one party is in the United States and the acquisition occurs in the United States.[59]

(2) Radio Intercepts. Intentional acquisition by a surveillance device of a radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both sender and all intended recipients are located in the United States. This covers surveillance of wire communications while they are transmitted over radio-microwave links. International radio-

---

[56]S. Rep. 660, 98th Cong., 2d Sess. (1984).

[57]S. Rep. 660, 98th Cong., 2d Sess. at 23.

[58]S. Rep. 660, 98th Cong., 2d Sess. at 3 and 4.

[59]50 U.S.C. § 1801(f)(2).

microwave communications are not covered by the FISA.[60] If domestic radio-microwave communications are acquired "intentionally," the contents must be destroyed upon recognition unless they indicate a threat of death or serious bodily harm.[61]

(3) Monitoring devices. Installation or use of a surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Such devices may include microphone eavesdropping, surreptitious closed-circuit television monitoring, transmitters that track movements of vehicles, and other techniques.[62] In some cases, the question of whether a device is covered by the FISA depends on the circumstances of its installation or use.[63]

(4) Watch listing. Acquisition by a surveillance device of the contents of wire or radio communications sent by, or intended to be received by, a particular known US person who is in the United States, if the contents are acquired by intentionally targeting that person under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Such targeting may involve acquisition of the contents of international communications of US persons.[64]

b. If a technique is on the borderline of the definition of electronic surveillance in the FISA, the issue is resolved following any precedents established by the FISA Court[65] (if there are conflicting decisions by other federal courts in criminal cases). The FISA does not cover electronic surveillance of US persons who are abroad, nor does it apply to "watch-listing" that targets the international communications of foreign nationals who are in the United States.[66] Moreover, the FISA does not apply to physical search techniques that would require a warrant for law

---

[60]50 U.S.C. § 1801(f)(3).

[61]50 U.S.C. §1806(i).

[62]50 U.S.C. § 1801(f)(4).

[63]See e.g., infra ¶ 5-8. Compare infra ¶ 6-19.

[64]50 U.S.C. § 1801(f)(1).

[65]See infra ¶¶ 4-7 and 4-8.

[66]Notwithstanding the limitations in the electronic surveillance of the FISA, all DoD intelligence electronic surveillance activities conducted for foreign intelligence or counterintelligence purposes are regulated under the purview of DoD 5240.1-R, Procedure 5.

enforcement purposes and do not fit the FISA definition of electronic surveillance. Such other intrusive techniques are not authorized by statute for intelligence purposes, but may be used under procedures approved by the Attorney General pursuant to E.O. 12333.[67]

c. The National Security Agency and the Federal Bureau of Investigation are the two principal agencies that employ electronic surveillance under the FISA. Certain activities covered by the FISA have also been conducted by the Central Intelligence Agency (CIA), DoD, and the Secret Service.[68] The CIA is precluded by executive order from engaging in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance.[69] The Secret Service performs defensive "sweeps" that may meet the definition of electronic surveillance under the FISA. As with testing and training, a special provision of the FISA permits such surveillance, under procedures approved by the Attorney General. These techniques may not be targeted against the communications of any particular person, and information acquired through a "sweep" may be used only to enforce Title III of the Omnibus Crime Control

---

[67]See e.g. DoD 5240.1-R and USSID 18 and infra ¶ 8-9b, note 19. See also 18 U.S.C. §§ 2510-2520, Wire Interception and Interception of Oral Communications (Title III, Omnibus Crime Control and Safe Streets Act of 1968), and Military Rules of Evidence, Rule 317, both of which prescribe conditions under which an application for warrant, or search authorization, may be submitted. There are a few rare circumstances in which the requirement for a warrant "if undertaken for law enforcement purposes" will differ from hypothesized circumstances for foreign intelligence or counterintelligence purposes. For example, under FISA § 102(a)(1) [50 U.S.C. § 1802(a)(1)], the President, through the Attorney General, may authorize electronic surveillance without a warrant to acquire foreign intelligence information when such surveillance is limited to the exclusive communications of foreign powers and there is no substantial likelihood that the surveillance will acquire the contents of any communication of a US person. Parties to these types of communications presumably are not entitled to the full protection of the Fourth Amendment to the Constitution. Title III contains no such discretionary executive authority.

Although the juxtaposition of the FISA and Title III on this issue is not entirely clear, it appears that where electronic surveillance is undertaken for law enforcement purposes, compliance with Title III would be required, regardless of the status of the target -- so long as the target were located within the territorial jurisdiction of the United States. On the other hand, if the electronic surveillance were for foreign intelligence or counterintelligence purposes, Title III would not apply. This raises the nearly irreconcilable issue of where the line is drawn between counterintelligence and criminal activities in so far as the crimes of espionage, et al, are concerned. It would appear that in many circumstances, the collecting intelligence component has a certain measure of latitude in selecting whether to proceed under the FISA or Title III.

[68]S. Rep. 660, 98th Cong., 2d Sess. 4 (1984).

[69]E.O. 12333, Pt. 2.4(a).

and Safe Streets Act of 1968[70] or section 605 of the Communications Act of 1934,[71] or to protect information from unauthorized surveillance.[72]

4-7. DESIGNATING FISA JUDGES. Under the FISA, the Chief Justice of the United States Supreme Court designates seven United States District Court judges, each of whom will hear applications for and grant orders (i.e., warrants) approving electronic surveillance under the Act. The Act further provides for the Chief Justice to designate three additional judges from the United States District Courts, or Courts of Appeals, to sit as a special appellate court to hear appeals by the United States from denials of applications made by any one of the seven District Court judges. Finally, under the FISA the Government may further appeal denials from this special appellate court to the United States Supreme Court.[73]

4-8. THE FISA COURT. The "FISA Court," that is the seven District Court judges and the special appellate court, has been quite active over the years. The total number of applications approved by the FISA Court in the last sixteen years has approached 9,200, for an average of approximately 550-575 per year.[74]

4-9. OBTAINING FISA WARRANTS. DoD obtains its FISA warrants, just as other federal agencies, through the Attorney General of the United States. All DoD requests must be cleared with the DIA General Counsel prior to submission, and must be submitted through the DoD GC to the Attorney General.[75] More about that later.

---

[70]50 U.S.C. §§2510-2520.

[71]47 U.S.C. §605.

[72]50 U.S.C. §1805(f)(2).

[73]50 U.S.C. § 1803.

[74]Office of Intelligence Policy Review, US Department of Justice.

[75]DoD 5240.1-R, Procedure 5, Pt. 1, §B.2.

Section III

Understanding the Terms

4-10. ELECTRONIC SURVEILLANCE.

a. As with all parts of the regulation, an understanding of the terminology used in DoD 5240.1-R, Procedure 5, is essential to an understanding of the policies, procedures and restrictions applicable to DoD intelligence component electronic surveillance activities. The most important and sometimes most confusing term to understand within the context of Procedure 5 is electronic surveillance.

b. The term electronic surveillance is one of the most elusive terms in DoD 5240.1-R, elusive in the sense that it seductively seems to be narrowly confined to just two specific situations, both involving nonconsensual acquisition of nonpublic communications -- one electronic, the other nonelectronic. DoD 5240.1-R, Appendix A, defines electronic surveillance as:

> 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 nonelectronic communication, without the consent of a person who is visibly present at the place of the communication...[76]

4-11. REASONABLE EXPECTATION OF PRIVACY.

a. The difficulty that exists in grappling with this definition lies in the lack of specificity regarding the meaning of "nonpublic." The route to that specificity requires an analysis of the Constitutional principles regarding the concept of a person's reasonable expectation of privacy.[77]

b. A nonpublic communication then, is one in which all the parties to that communication hold a reasonable expectation that the contents of that communication will remain private. Most -- but not all -- telephone conversations are nonpublic communications. For example, for the purposes of electronic surveillance, conversations on the DoD telephone system are nonpublic, even though notice has been given to all users of the system that calls on DoD telephones are subject to communication security monitoring. By that notice, users of the system, through the voluntary act of using a DoD telephone are deemed to have consented to communica-

---

[76]DoD 5240.1-R, Appendix A, ¶ 9.

[77]See infra § IV.

tions security monitoring of their calls.[78] This consent is limited, however, and does not extend to monitoring for other purposes, such as foreign intelligence or counterintelligence. Thus, for all purposes except communications security monitoring, conversations on the DoD telephone system are protected.

4-12. FLUIDITY OF THE LAW. This area of the law, defining the limits to the concept of reasonable expectation of privacy, is fairly fluid -- although some basic principles are settled. Most importantly, where there has been consent to monitoring of a conversation or acquisition of its contents, the essential element of a reasonable expectation of privacy for all the parties to the communication has been invalidated, and the warrant requirements of the law no longer apply.[79]

4-13. SUMMARY.

To sum up this section of our discussion, you should understand that within the context of DoD 5240.1-R, Procedure 5, where the term electronic surveillance is used, it is derived from the use of the term in the FISA, E.O. 12333 and DoD 5240.1-R, and it generally means nonconsensual electronic surveillance.

---

[78]See DoD 5240.1-R, Telephone Communications Security Monitoring.

[79]DoD 5240.1-R, Procedure 5, Pt. 2, § A.

Section IV

What Constitutes a "Reasonable Expectation of Privacy"?

4-15. THE FOURTH AMENDMENT. The concept of reasonable expectation of privacy in electronic surveillance is derived directly from decisions of the United States Supreme Court in cases involving searches and seizures under, or in violation of an individual's rights flowing from the Fourth Amendment to the Constitution of the United States. The Fourth Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

4-16. AMENDMENT PROTECTS PEOPLE - NOT PLACES. It has long been held that the principal object of the Fourth Amendment is the protection of privacy, and that the Amendment protects people, not places. In 1968, the Supreme Court of the United States said --

> Capacity to claim the protection of the Amendment depends not upon a property right in the invaded place, but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion.[80]

4-17. EXAMPLES OF COURT HOLDINGS. Over the years, the courts have made numerous rulings regarding the governmental conduct and the individual's expectation of privacy. The following characterizations generally represent the areas where the courts have defined the limitations of governmental power in electronic surveillance matters; however, because of the constant changing of the law in this area, a legal review of the applicable facts and circumstances should be obtained before proceeding or discarding a particular approach.

a. General.

(1) Use of spike microphone - warrant required under Fourth Amendment.[81]

---

[80]Mancusi v. DeForte, 392 U.S. 364, 368 (1968).

[81]Silverman v. United States, 365 U.S. 505 (1961).

(2) Radio broadcast communications - no reasonable expectation of privacy.[82]

b. Consensual surveillance.

(1) Warrant for "wired" informant not required by Fourth Amendment.[83]

(2) Conversations obtained with consent of a party - not subject to warrant requirement.[84]

c. Beepers.

(1) Installation of beeper in a container with consent of present owner but without consent of person to whom container is delivered - not a search or seizure within meaning of Fourth Amendment.[85]

(2) No warrant necessary for the placing of beeper in container later sold to defendant and for use of beeper to monitor defendant's travel on public roads -- defendant had no expectation of privacy in travels on public roads.[86]

(3) Warrant not required to use beeper in airplanes and failure to remove beeper prior to expiration of warrant did not require suppression - no reasonable expectation of privacy in flying airplane.[87]

(4) No warrant necessary for beeper on exterior of automobile - beeper must be "turned off" when automobile enters area where reasonable expectation of privacy exists (e.g., owner's garage).[88]

---

[82]United States v. Hall, 488 F.2d 193 (9th Cir. 1973).

[83]United States v. White, 401 U.S. 745 (1971), reh'g denied, 402 U.S. 990 (1971), on remand, 454 F.2d 435 (7th Cir. 1971), cert denied, 406 U.S. 962 (1972).

[84]Rathbun v. United States, 355 U.S. 107 (1957), reh'g denied, 355 U.S. 925 (1958).

[85]United States v. Karo, 468 U.S. 705, reh'g denied, 468 U.S. 1250 (1984).

[86]United States v. Knotts, 460 U.S. 276 (1983).

[87]United States v. Butts, 729 F.2d 1514 (5th Cir. 1984) (en banc), cert. denied, 469 U.S. 855 (1984) and 476 U.S. 1140 (1986).

[88]United States v. Michael, 645 F.2d 252 (5th Cir. 1981), cert. denied, 454 U.S. 950, reh'g denied, 454 U.S. 1117 (1981).

d. Video.

Video surveillance - warrant required if reasonable expectation of privacy to space under surveillance.[89]

e. Pen registers.

No reasonable expectation of privacy - warrant not required by Fourth Amendment.[90] (Some state constitutions, e.g., Colorado[91], require a warrant for the use of a pen register).

f. Radio communications and cordless telephones.

(1) Cordless telephone communication, not "wire communication" - user has no reasonable expectation of privacy.[92]

(2) No expectation of privacy in radio communications received by ordinary receivers - even if encryption or other deception used.[93]

---

[89]United States v. Humphrey, 456 F.Supp. 51 (E.D. Va. 1978), aff'd, United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980), appeal after remand, United States v. Hung, 667 F.2d 1105 (4th Cir. 1981), cert. denied, Truong Dinh Hung v. United States, 454 U.S. 1144 (1982).

[90]Smith v. Maryland, 442 U.S. 735 (1979).

[91]People v. Sporleder, 666 P.2d 135 (Colo. 1983).

[92]State v. Howard, 679 P.2d 197, (Kan. 1984).

[93]United States v. Rose, 669 F.2d 23 (1st Cir. 1982), cert. denied, 459 U.S. 828 (1982).

Section V

The Regulatory Framework of Electronic Surveillance

4-18. GENERAL.

a. As you have probably already surmised, the regulatory framework of Procedure 5 is divided into the following general categories: non-emergency and emergency situations; situations which occur within and outside the United States; and finally, activities which affect US persons and non-US persons.

b. The levels of approval authority, the authority to approve requests, and the case approval standards for these various electronic surveillance activities are complex and frequently difficult to follow within the context of DoD 5240.1-R, Procedure 5. See table 4-1.[94]

4-19. APPROVAL ALWAYS REQUIRED.

a. The first important point to note is that for the purposes of DoD intelligence operations, absolutely no electronic surveillance activity may be carried out within the United States against US or non-US persons, without US Attorney General approval.[95] The next point to note is that Procedure 5 requires a strong showing for approval of electronic surveillance in the United States. Even in emergency circumstances, all such requests must be cleared through the DoD General Counsel and approved by the Attorney General of the United States (signals intelligence activities, which are discussed in the next section, are coordinated through the National Security Agency to the Attorney General). On the other hand, electronic surveillance directed against a US person abroad may be authorized by any general or flag officer at the overseas location in question having responsibility for either the subject of the electronic surveillance or protection of the endangered persons, installation, or property.

b. It must be emphasized that securing approval of electronic surveillance either within or outside the United States, even against US persons, when required for legitimate, justified intelligence or counterintelligence operations is not an extraordinary task. In fact, in most cases the procedures involved in securing approval require little more effort than otherwise involved in processing and coordinating an operations plan.

---

[94]Table 4-1 organizes and displays this complicated regulatory and legal framework into a consolidated matrix format.

[95]Neither E.O. 12333 nor DoD 5240.1-R place constraints on "consensual" electronic surveillance or electronic surveillance against a non-US person outside the United States.

Frequently, the surveillance approval process may require only one or two more steps. Furthermore, where the exigencies of the situation warrant, officials involved in the coordination and approval chain are prepared to quickly address the substance of a particular request and are sensitive to the need to avoid imposing unnecessary administrative burdens on intelligence operations.

4-20. APPROVAL AUTHORITIES.

a. Within the United States, requests to conduct electronic surveillance for intelligence purposes are governed by the FISA. All requests by DoD intelligence components for such authority must conform to the procedures in Procedure 5, part 1, section B, and are to be submitted through command channels to the DIA GC for submission to the DoD General Counsel. Applications for FISA Court orders are then processed in legal channels through the Attorney General, after prior clearance by the General Counsel of the Department of Defense.

b. Outside the United States, electronic surveillance directed against US persons abroad requires the same approvals described immediately above.[96] (See table 4-1.)

c. Finally, electronic surveillance of non-US persons abroad is not governed by DoD 5240.1-R and may be authorized under service authority.

4-21. APPROVAL STANDARDS.

a. The standards for approval of electronic surveillance activities vary according to the relative intrusiveness of the activity, and the status of the target of the surveillance. In all cases of electronic surveillance directed against US persons it must be shown that the information sought cannot be reasonably obtained by some less intrusive means.[97]

b. US persons in the United States are entitled to the full protection of the Fourth Amendment, and any surveillance in those circumstances must be supported by a probable cause showing that the target is an agent of a foreign power, or acting in some capacity for a foreign power, international terrorist organizations, or the like. Electronic surveillance in these cases must be preceded by the issuance of a FISA Court order, or approval by the Attorney General of the United States, pending securing such a warrant within 24 hours.[98]

---

[96]DoD 5240.1-R, Procedure 5, Pt. 2, § E.

[97]DoD 5240.1-R, Procedure 5, Pt. 2, § C.2.b.

[98]50 U.S.C. § 1804.

c. The system is complex, but it is not impossible. Its underlying structure is designed to balance the legitimate needs of the government with the rights of the individual. Given those constraints, one could not expect a system to exist which did not inherently contain adequate checks, balances, and oversight procedures.

4-22. CONTROL AND RETENTION PROCEDURES. One final point about this regulatory framework. Procedure 3 covers the control and retention of electronic surveillance information. All electronic surveillance information acquired through DoD intelligence operations or received from cooperating sources is subject to these control and retention procedures, and those persons who are responsible for handling such information must become familiar with those sections in DoD 5240.1-R, Procedure 3.[99]

[99]See also FISA § 106 (50 U.S.C. § 1806) which required minimization procedures for control and dissemination of electronic surveillance information. Army implementation of § 106 is contained in DoD 5240.1-R, Procedure 3, § E.

Table 4-1
Approval of electronic surveillance, DoD 5240.1-R, Procedure 5

GENERAL RULE: No DoD intelligence component may conduct electronic surveillance directed against a US person without first securing approval from a properly designated approval authority.

ELECTRONIC SURVEILLANCE ACTIVITY	FISA 1/ YES/NO	APPROVAL 2/ AUTHORITY	APPROVAL STANDARDS
1. Within the United States			
a. Non-Emergency Situations			
(1) US persons	YES	Note A1	Note B1
(2) Non-US persons	YES	Note A2	Note B2
b. Emergency Situations			
(1) US persons	YES	Note A2	Note B1
(2) Non-US persons	YES	Note A2	Note B2
2. Outside the United States			
a. Non-Emergency Situations			
(1) US persons	YES	Note A2	Note B3
(2) Non-US persons	NO	None	None
b. Emergency Situations			
(1) US persons	YES	Note A4 & Note A5	Note B5
(2) Non-US persons	NO	None	None

Table 4-1
Approval of electronic surveillance, DoD 5240.1-R, Procedure 5

FOOTNOTES:

1/ Foreign Intelligence Surveillance Act of 1978. This item indicates whether the listed activity is subject to the provisions of the FISA.

2/ The authority to approve the submission of applications for requests for electronic surveillance under the FISA is limited to the Secretary or Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency.

NOTES:

A. Case Approval Authorities. The authorities listed here apply to the approval of the electronic surveillance activity which is the object of a particular request.

1. Foreign Intelligence Surveillance Court, which was established pursuant to the Foreign Intelligence Surveillance Act of 1978, to hear applications for and grant orders approving electronic surveillance for intelligence purposes.

2. The Attorney General of the United States, who is the cabinet-level Executive Branch Official, who heads the United States Department of Justice.

3. The Secretary or Deputy Secretary of Defense; the Secretary or Under Secretary of a Military Department; or the Director, National Security Agency.

4. A 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 persons, installations, or property that is endangered; or the Deputy Director for Operations, National Security Agency.

Table 4-1
Approval of electronic surveillance, DoD 5240.1-R, Procedure 5

5. The Secretary or Under Secretary of a DoD department, or the DoD General Counsel.

B. Case Approval Standards.

1. Probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power, and that each of the targeted facilities or places is about to be used by a foreign power or an agent of a foreign power. Orders issued pursuant to this authority will be limited in duration by the FISA Court.

2. Certification in writing by the Attorney General of the United States that the target of the electronic surveillance is communication exclusively between and among foreign powers, and that the targeted premises are under open and exclusive control of a foreign power. In these circumstances, authorization may be granted by the Attorney General for up to one year without a FISA Court order.

3. Electronic surveillance must be necessary to obtain significant foreign intelligence or counterintelligence information that could not be obtained by other less intrusive collection techniques, and there must be probably cause to believe that the target of the electronic surveillance is one of the following:

a. A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities, sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaged in such activities;

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

c. A person unlawfully acting for, or pursuant to the direction of, a foreign power;

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

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

Table 4-1
Approval of electronic surveillance, DoD 5240.1-R, Procedure 5

4. Electronic surveillance in these circumstances may be conducted to support any lawful function assigned to the requesting DoD intelligence component, provided the approval authority determines that a reasonable belief exists that the surveillance will gather valuable intelligence information.

5. Exercise of approval authority in these circumstances is limited to cases where securing approval of the Attorney General is not practical because:

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

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

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

Section VI

Signals Intelligence Activities

4-23. THE UNITED STATES SIGINT SYSTEM.

a. Certain elements of the DoD are part of the United States Signals intelligence system, or the "US SIGINT System" as it is called. The US SIGINT System is the unified organization for SIGINT activities under the direction of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). It is comprised of the NSA/CSS, the components of the military services authorized to conduct SIGINT activities, and certain other activities authorized by the National Security Council or the Secretary of Defense to conduct SIGINT collection, processing and/or dissemination activities.

b. All SIGINT operations by the US SIGINT System are conducted under the authority of the DIRNSA/CHCSS, who is authorized to and maintains direct contact with the Attorney General of the United States for the purposes of securing emergency approval of electronic surveillance (i.e., nonconsensual) under the FISA, and for the purposes of securing warrants from the FISA Court. See table 4-2.

4-24. DEFINITION OF SIGINT. DoD 5240.1-R defines SIGINT as --

> A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combinations.[100]

4-25. "GENERIC" SIGINT. Nice definition, but what does it mean in the context of the electronic surveillance procedures of DoD 5240.1-R? "Generic" SIGINT is a broad category of intelligence which includes, but is not limited to, nonconsensual electronic surveillance.

a. Electronic surveillance, as we have already discussed, involves the acquisition of nonpublic communications without the consent of a party to the communication, or without the consent of a person who is visibly present at the place of communication. SIGINT, on the other hand, encompasses much more than nonpublic communications. It includes the interception of public communications signals and of other noncommunications electronic signals.

b. However, for the purposes of SIGINT activities under the regulatory and statutory framework, i.e., DoD 5240.1-R, E.O. 12333

---

[100]DoD 5240.1-R, Appendix A, ¶ 23.

and the FISA, Procedure 5 only governs certain electronic surveillance activities. Specifically, it covers only those --

> ...signals intelligence activities that involve the collection, retention, and dissemination of foreign communications and military tactical communications.[101]

c. Procedure 5 **DOES NOT** apply to SIGINT activities to collect public communications and noncommunications electronic signals.

4-26. INCIDENTAL ACQUISITION OF INFORMATION ABOUT US PERSONS. Because SIGINT collection activities are so extensive, they may incidentally involve the acquisition of information concerning US persons without their consent, and the intercept of communications originated or intended for receipt in the United States, without the consent of a party to the communication. Because of the pervasive difficulty, if not impossibility, in discriminating between signals in such a manner as to preclude "electronic surveillance" of US persons, the underlying regulatory control system reaches to and controls all SIGINT activities that may incidentally involve the collection of information concerning US persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of all the parties to the particular communication.[102]

a. For the purposes of SIGINT, communications concerning a US person are those in which a US person is identified in the communication. A US person is identified when that 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.[103]

b. In addition, for the purposes of SIGINT activities only, the following guidelines apply in determining whether a person is a US person:[104]

(1) A person known to be currently in the United States will be treated as a US person unless the nature of the person's communications or other available information concerning the person

---

[101]DoD 5240.1-R, Procedure 5, Part 3, § A.1.

[102]DoD 5240.1-R, Procedure 5, Part 3, § A.1.

[103]DoD 5240.1-R, Procedure 5, Part 3, § B.1. A reference to a product by brand name or manufacturer's name, or the use of a name in a descriptive sense (e.g., Monroe Doctrine), is not an identification of a US person.

[104]DoD 5240.1-R, Procedure 5, Part 3, § B.4.

give rise to a reasonable belief that such a person is not a US citizen or permanent resident alien.[105]

(2) A person known to be currently outside the United States, or whose location is not known, will not be treated as a US person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such a person is a US citizen or permanent resident alien.[106]

(3) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a US 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.[107]

(4) An unincorporated association whose headquarters are located outside the United States may be presumed not to be a US person unless the collecting component has information indicating that a substantial number of members are citizens of the United States or permanent resident aliens.[108]

4-27. APPLICABILITY OF THE FISA TO SIGINT. In addition, the applicable law, the Foreign Intelligence Surveillance Act (FISA), applies to any SIGINT activity involving communications sent to or from the United States in which the communicants have a reasonable expectation of privacy; to any wiretap for SIGINT purposes in the United States; to the acquisition of private radio signals where all communicants are located in the United States; and to the use of SIGINT devices within the United States.

4-28. CONTROL AND OVERSIGHT OF SIGINT OPERATIONS. The policies and procedures for the control and oversight of SIGINT operations are contained in the various US SIGINT System Directives (USSID) pertaining to SIGINT activities and organizations within the US

---

[105]Compare supra ¶ 3-10.

[106]Compare supra ¶ 3-10a.

[107]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. DoD 5240.1-R, Procedure 5, Pt. 3, § B.4.c.

[108]See DoD 5240.1-R, Appendix A, ¶ 25b, which states that an "organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained." This presumption seems of no substantive difference from that permitted for SIGINT activities. Perhaps this provision in the SIGINT guidelines (DoD 5240.1-R, Procedure 5, Part 3, § B.4.d.) is a distinction without a difference.

SIGINT System. General guidance is published in USSID 18, the distribution of which is strictly controlled and limited to those organizations within the US SIGINT System which have a need-to-know of its contents. Suffice it to say that any and all SIGINT collection activities within the DoD must be done in accordance with USSID 18, and must follow the operational and technical control instructions of the DIRNSA/CHCSS.

a. The fact that a DoD element is part of the US SIGINT System does not relieve the DoD element of its control and oversight responsibilities. Commanders and oversight personnel must assure that all operational activities of the element are in compliance with the applicable provisions of DoD 5240.1-R and USSID 18.

b. In addition, the familiarization requirements of DoD 5240.1-R, Procedure 14, apply. Personnel of the US SIGINT System must be familiar with the provisions of DoD 5240.1-R, Procedures 1 through 5 and 15, and USSID 18.[109]

[109]DoD 5240.1-R, Procedure 14, § B.2. See ¶ 8-15, infra.

Table 4-2
Signals intelligence activities, DoD 5240.1-R, Procedure 5

GENERAL RULE: The interception,1/ retention and dissemination of communications 2/ concerning US persons 3/ by DoD intelligence components of the US SIGINT System is governed by USSID 18 and DoD 5240.1-R, and is subject to certain restrictions and limitations. 4/

	RESTRICTIONS AND LIMITATIONS
1. Foreign communications.	May collect, process, retain and disseminate only in accordance with USSID 18.
2. Military tactical communications. 5/	May collect, process, retain and disseminate only in accordance with USSID 18 and the following: a. Collection efforts must be designed to the extent feasible to avoid intercept of communications not related to military exercises. b. Communication intercepts of US persons not participating in the exercise that are inadvertently intercepted during the exercise must be destroyed as soon as feasible. c. Exercise reports or information files must be limited in their dissemination to those persons and authorities participating in or conducting critiques and reviews of such exercise.

NOTES:

1/ Interception means the acquisition by the US SIGINT 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. This does not include the display of signals on visual display devices intended to permit examination of the technical characteristics of the signals without reference to the information content carried by the signals.

2/ For the purposes of SIGINT, communications concerning a US person are those in which a US person is identified. A US person is identified when that 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.

Table 4-2
Signals intelligence activities, DoD 5240.1-R, Procedure 5

3/ For SIGINT activities purposes only, the following guidelines apply in determining whether a person is a US person:

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

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

c. A person known to be an alien admitted for permanent residence may be assumed to have lost status as a US 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.

d. An unincorporated association whose headquarters are located outside the United States may be presumed not to be a US person unless the collecting component has information indicating that a substantial number of members are citizens of the United States or permanent resident aliens.

4/ SIGINT activities conducted under the operational and technical control of the DIRNSA/CHCSS which involve communications of non-US persons are not subject to the restrictions and limitations of either DoD 5240.1-R or USSID 18; however, any incidental acquisition of information concerning US persons, regardless of the target of the underlying collecting, is subject to both USSID 18 and DoD 5240.1-R restrictions and limitations. Further, SIGINT activities conducted by DoD intelligence components and not under the operational and technical control of the DIRNSA/CHCSS are subject to electronic surveillance controls, standards and procedures of DoD 5240.1-R.

5/ Military tactical communications means United States and allied military exercise communications within the United States and abroad necessary for the production of simulated counterintelligence and foreign intelligence or to permit an analysis of communications security.

Section VII

Technical Equipment and Training Activities

4-29. GENERAL. DoD 5240.1-R, Procedure 5, contains four additional parts which address the control of technical matters related to the use of electronic surveillance equipment, training personnel in the use of that equipment, and the use of certain communications and noncommunications signals for training, equipment testing, research and development, and equipment calibration. These are:

a. Part 4 - Technical Surveillance Countermeasures.[110]

b. Part 5 - Developing, Testing, and Calibration of Electronic Equipment.[111]

c. Part 6 - Training of Personnel in the Operation and Use of Electronic Surveillance Equipment.[112]

d. Part 7 - Conduct of Vulnerability and Hearability Surveys.[113]

4-30. REGULATION AND OVERSIGHT OF TECHNICAL ACTIVITIES.

a. The inclusion of these technical matters within the regulatory and oversight framework for electronic surveillance is demonstrative of the broad reach of that system, and of the commitment by proponents of the system (i.e., the Congress, the President, etc.) to the dual principles of preservation of the Fourth Amendment rights against governmental intrusion, and the legitimacy of necessary intelligence and counterintelligence operations.

b. Discussion in detail of the regulatory procedures affecting these technical activities is beyond the scope of this handbook. Therefore, we will confine our discussion to a brief description of each activity, and a display of the general rules affecting each. DoD personnel who are directly involved in any of those particular technical areas of electronic surveillance must seek additional, more detailed information, to assure an under-

---

[110]DoD 5240.1-R, Procedure 5, Part 4. See FISA § 105(f)(2), 50 U.S.C. § 1805(f)(2).

[111]DoD 5240.1-R, Procedure 5, Part 5. See FISA § 105(f)(1), 50 U.S.C. § 1805(f)(1).

[112]DoD 5240.1-R, Procedure 5, Part 6. See FISA § 105(f)(3), 50 U.S.C. § 1805(f)(3).

[113]DoD 5240.1-R, Procedure 5, Part 7.

standing of the constraints and the permissible limits on their mission activities.

4-31. TECHNICAL SURVEILLANCE COUNTERMEASURES.

a. Technical surveillance countermeasures, or TSCM, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance activities being attempted by unauthorized persons, and for determining the susceptibility of electronic equipment to such unlawful electronic surveillance. TSCM are those measures used to detect the present of "bugs", "wiretaps", or other unauthorized surveillance devices, and for DoD 5240.1-R purposes, TSCM includes some of the measures used in detecting compromising emanations of electronic equipment.

b. TSCM activities may be undertaken only following the authorization or consent of the official or commander in charge of the installation, facility or organization which is the object of such services. When undertaken, TSCM services must be limited in duration to the minimum time required to accomplish the specific TSCM mission, and access to the informational content of communications acquired during any particular TSCM activity must be strictly controlled. Limitations pertaining to TSCM activities are shown in table 4-3.

4-32. DEVELOPING, TESTING AND CALIBRATING EQUIPMENT. The regulation of activities pertaining to developing, testing, and calibrating electronic equipment under DoD 5240.1-R reaches to the protection of communications signals in the laboratory environment. The parameters of signals and types of signals which may be used are limited in such a manner as to assure the protection of any communicants' reasonable expectations of privacy - even where use and acquisition of the underlying signals carrying those protected conversations is in a laboratory context. Table 4-4 displays these rules and restrictions.

4-33. TRAINING ACTIVITIES. The training of personnel in the operation and use of electronic communications and surveillance equipment is also regulated by DoD 5240.1-R. Procedure 5 covers three specific areas: training guidance, training limitations, and the retention and dissemination of information collected during training. Table 4-5 contains an outline of those regulatory procedures and limitations.

4-34. VULNERABILITY AND HEARABILITY SURVEYS.

a. The conduct of vulnerability and hearability surveys is the final regulatory topic of DoD 5240.1-R, Procedure 5. These surveys are signals security (SIGSEC) assessment techniques and are to be used only for communications security (COMSEC) purposes.

(1) Vulnerability surveys refer to acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.

(2) Hearability surveys refer to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the quality of reception over time.

b. The procedures and limitations affecting the conduct of vulnerability and hearability surveys are shown in table 4-6.

c. Hearability surveys which concern communications signals originated outside the territorial jurisdiction of the United States are not covered by Procedure 5, provided adequate measures exist to preclude monitoring of communications of or concerning US persons.

Table 4-3
Technical surveillance countermeasures controls, DoD 5240.1-R, Procedure 5

GENERAL RULE: TSCM activities which may involve the incidental acquisition of nonpublic communications of US persons, without their consent, are subject to several limitations and restrictions. 1/

	LIMITATIONS AND RESTRICTIONS	
1.	Authorization required for TSCM activities.	Must be approved by the official in charge of the facility, organization or installation where the TSCM services are to be performed.
2.	Scope permitted in TSCM activities.	Limited in extent and duration to that necessary to determine existence and capability of any unauthorized surveillance equipment.
3.	Limitations on access to content of communications acquired during TSCM activities.	1. Limited to persons involved directly in conducting services. 2. Content acquired must be destroyed as soon as practical or upon completion of the TSCM activity.
4.	Use, retention, or dissemination of US person information. 2/	1. Approval. Must be approved by service Secretary or service Under Secretary; in emergency situations by a DoD flag or general officer. 2. Justification required. a. Any location. Clear and imminent threat to life or property - may pass to law enforcement authorities. b. Within the US. A, above, and only as necessary in protecting against unauthorized surveillance, or involving federal felony violations. c. Outside the US. A and B, above, and any information indicating UCMJ or other federal law violation may be used, retained or disseminated.

NOTES:

1/ The intentional acquisition of nonpublic communications of US persons, without their consent, is not permitted in connection with TSCM activities, unless approved as nonconsensual electronic surveillance. See table 4-1.

2/ The limitations described here are derived from the provisions of section 105(f)(2)(c) of the Foreign Intelligence Surveillance Act [50 U.S.C. § 1805(f)(2)(c), as amended], which states that any information concerning US persons acquired by TSCM activities shall be used only to enforce Title 18, United States Code, chapter 119, (18 U.S.C. § 2510, et. seq.) or section 605 of the Communications Act of 1934 (47 U.S.C. § 605).

Table 4-4
Developing, testing and calibrating equipment, DoD 5240.1-R, Procedure 5

GENERAL RULE: Technical communications data (i.e., frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for developing, testing or calibrating electronic equipment; collection avoidance purposes; or research and development on signal sources. 1/

SIGNALS AND RESTRICTIONS ON USE	
1. Signals authorized for use without restrictions.	1. Laboratory-generated signals. 2. Communications signals with the consent of the communicator. 3. Communications in commercial or public service broadcast bands. 4. Communications transmitted between terminals located outside US not used by known US persons. 5. Noncommunications signals (including telemetry and radar).
2. Communications signals acquired subject to lawful electronic surveillance authorizations.	May be used subject to the minimization procedures applicable to such electronic surveillance. 2/
3.a. Communications signals over official government circuits with consent from appropriate official of the controlling agency. b. Communications signals in citizens and amateur radio bands.	1. Scope and duration of surveillance limited to that necessary for purposes stated in general rule above. 2. No particular US person may be targeted intentionally without consent. 3. Content of communication may be: a. Retained only when actually needed for a purpose stated in the general rule, above. b. Disseminated only to persons conducting the activity; and c. Destroyed immediately upon completion of the activity.
4. Other signals upon determination that it is not practical to use above signals or it is not reasonable to obtain consent.	Same as above for up to 90 days. Attorney General must approve the test proposal for periods in excess of 90 days.

NOTES:

1/ These limitations on testing electronic equipment are derived from section 105(f)(1) of the Foreign Intelligence Surveillance Act [50 U.S.C. § 1805(f)(1)].

2/ Minimization procedures are those restrictions imposed on the dissemination of information lawfully possessed by an agency and acquired by electronic surveillance.

Table 4-5
Training personnel to use surveillance equipment, DoD 5240.1-R, Procedure 5

GENERAL RULE: Training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment is subject to certain procedures and limitations. 1/

	PROCEDURES AND LIMITATIONS
1. Training curriculum.	Must include guidance concerning requirements and restrictions of the Foreign Intelligence Surveillance Act and E.O. 12333 regarding unauthorized use of US persons communications.
2. Use of equipment and acquisition of information by electronic surveillance means. 2/	1. No restrictions on public broadcasts and distress signals. 2. US Government communications may be monitored - consent is required from an appropriate official. 3. Minimal acquisition is permitted to calibrate equipment. 4. Use of electronic communications and surveillance equipment permitted under these conditions: a. To maximum extent practical, must be directed against communications subject to lawful electronic surveillance. b. Aural acquisition of private communication not permitted without consent or approval. c. Surveillance must be limited in extent and duration to that needed for specific training.
3. Retention and dissemination of information collected during training.	1. Where communications are those otherwise subject to lawful electronic surveillance, may be retained and disseminated subject to minimization procedures applicable to such activity. 3/ 2. Other information - destroy as soon as practical upon completion of the training involved.

NOTES:

1/ The rules, procedures and limitations on training intelligence personnel on the use of electronic surveillance equipment are derived in part from section 105(f)(3) of the Foreign Intelligence Surveillance Act [50 U.S.C. § 1805(f)(3)].

2/ Interception of communications for training purposes is also subject to the rules applicable to nonconsensual and consensual electronic surveillance. See table 4-1.

3/ Minimization procedures are those restrictions imposed on the dissemination of information lawfully possessed by an agency and acquired by electronic surveillance.

Table 4-6
Vulnerability and hearability surveys, DoD 5240.1-R, Procedure 5

GENERAL RULE 1: Nonconsensual surveys may be conducted to determine the potential vulnerability of transmission facilities to foreign intelligence services, only with the prior written approval of the Director, National Security Agency, or his designee.

	PROCEDURES AND LIMITATIONS
1. Aural acquisition (listening by human ear) of transmission.	Not permitted.
2. Acquisition of content of a transmission.	Not permitted.
3. Recording of transmission.	Not permitted.
4. Reports and logs.	May not identify US persons or entities except to the extent necessary to identify vulnerable transmission facilities.

GENERAL RULE 2: The Director, National Security Agency, may conduct, or authorize other agencies to conduct hearability surveys of telecommunications transmitted in the United States.

	LIMITATIONS
1. Collection of communications signals.	Where practical, consent must be secured from facility affected.
2. Processing and storage of communications signals.	1. Communications content not to be recorded or included in report. 2. No microwave transmission may be demultiplexed or demodulated for any purpose.
3. Reports and logs.	1. Reports and logs may not identify persons or entities except to identify the transmission facility that can be intercepted from a particular site. 2. Reports may be disseminated only within the US Government. 3. Logs to be disseminated only to verify reported results.

Section VIII

Conclusion

4-35. INDIVIDUAL RIGHTS.

a. Individual freedoms and privacy are fundamental in our society and to its preservation. While it is self-evident that constitutional government must be maintained, it is also fundamental, though less self-evident, that an effective and efficient intelligence system is necessary. And, to be effective, many intelligence activities must be conducted in secrecy, and many of the methods used must be intrusive upon the individual freedoms and privacy of subjects of investigations, sources of intelligence, and those associated with such subjects and sources.

b. Satisfying these objectives presents considerable opportunity for conflict. The vigorous pursuit of intelligence by certain methods, including those employed in electronic surveillance techniques, can lead to invasions of individual rights. The preservation of the United States requires an effective intelligence capability, but the preservation of individual liberties within the United States requires limitations or restrictions on some of the methods used in gathering intelligence. The drawing of reasonable lines - where legitimate intelligence needs end and erosion of Constitutional government begins - is difficult.

4-36. THE NEEDS OF NATIONAL SECURITY.

a. In seeking to draw such lines, we must be guided in the first instance by the commands of the Constitution as they have been interpreted by the Supreme Court, the laws as written by Congress and executed by the President, the values we believe are reflected in the democratic process, and the faith we have in this free society. We must also be fully cognizant of the needs of national security; the requirements of a strong national defense against external aggression, internal subversion, and international terrorism; and the duty of the government to protect its citizens.

b. In the final analysis, public safety and individual liberty sustain each other.

Chapter 5

CONCEALED MONITORING AND PHYSICAL SEARCHES

Section I

Introduction

5-1. GENERAL. The rules for concealed monitoring and physical searches, both of which are characterized under DoD 5240.1-R as "special collection techniques"[114] are covered in this chapter. Procedure 6 applies to concealed monitoring and Procedure 7 applies to physical searches.

5-2. USE OF SPECIAL COLLECTION TECHNIQUES. The use of concealed monitoring and physical searches, as with all special collection techniques, must be based upon a proper function assigned to the employing intelligence component[115], and must be preceded by a determination that the selection of one of these techniques amounts to the employment of the least intrusive lawful investigative means reasonably available to collect the required information.[116]

5-3. LIMITATION ON COLLECTION OF FOREIGN INTELLIGENCE. Where special collection techniques are employed in the United States, foreign intelligence concerning US persons may be collected only where the information sought is significant, coordination has been effected with the Federal Bureau of Investigation (FBI), and the use of other overt means has been approved by the head of the intelligence component concerned, or his or her single designee.[117]

5-4. JURISDICTION IN COUNTERINTELLIGENCE INVESTIGATIONS. Where counterintelligence investigations are involved, somewhat different jurisdictional rules apply. Coordination with the FBI is not required where the subject of the investigation is solely under the investigative jurisdiction of the DoD component. These include active duty military personnel and investigations of incidents involving reservists and National Guard members which occurred

---

[114]See supra chapter 3, § III.

[115]DoD 5240.1-R, Procedure 1, § A.1.

[116]DoD 5240.1-R, Procedure 2, § D. See supra table 3-2.

[117]DoD 5240.1-R, Procedure 2, § E.

while on active military duty.[118] Appendix B further details investigative jurisdiction over counterintelligence cases.

[118]Even though coordination may not be required, in most cases such coordination is appropriate to assure thoroughness of the results.

Section II

Procedure 6 - Concealed Monitoring

5-5. SCOPE OF PROCEDURE 6.

a. "Concealed monitoring" is the subject of DoD 5240.1-R, Procedure 6. It is important to note that the application of this procedure is confined to concealed monitoring --

> ...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...and no warrant would be required if undertaken for law enforcement purposes.[119]

b. Unless the concealed monitoring meets all of the above tests, it is not covered by Procedure 6. Now, that does not mean that there are no restrictions on monitoring activity. On the contrary, the absence of one of the above factors will probably signal the application of more, not less, restrictive rules than those prescribed in Procedure 6.

5-6. THE TESTS OF CONCEALED MONITORING. Let's look at each test in a little more detail.

a. First, for Procedure 6 to apply, the concealed monitoring must be undertaken for foreign intelligence or counterintelligence purposes. Put another way, DoD intelligence components may use concealed monitoring ONLY in connection with lawful operational activities designed to collect --

(1) FOREIGN INTELLIGENCE, which is information relating to capabilities, intentions, and activities of foreign powers, organizations, or persons[120]; or

(2) COUNTERINTELLIGENCE, which is information gathered to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities (but not including personnel, physical, document, or communications security programs information).[121]

---

[119]DoD 5240.1-R, Procedure 6, § A.1. Emphasis added.

[120]DoD 5240.1-R, Appendix A, ¶ 5.

[121]DoD 5240.1-R, Appendix A, ¶ 5.

b. Second, to be within the ambit of Procedure 6, concealed monitoring must be conducted within the United States or directed against a US person outside the United States.[122]

c. Concealed monitoring of non-US persons abroad is not subject to the restrictions and limitations of Procedure 6, and may be conducted for any lawful function assigned to the specific DoD intelligence component involved.

d. Next, the person who is the subject of concealed monitoring under Procedure 6 must not have a reasonable expectation of privacy in the activities to be monitored. (The concept of reasonable expectation of privacy was discussed in detail in chapter 4, section IV, of this handbook.) Whether a person has a reasonable expectation of privacy in a particular activity depends on the circumstances of each case.

5-7. CONSULTATION WITH LEGAL OFFICE.

a. Procedure 6 requires that this determination be made ONLY after consultation with the DoD legal office responsible for advising the intelligence component which proposes to conduct the concealed monitoring.[123] Within the context of Procedure 6, a 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.[124]

b. For example, the Supreme Court of the United States has held that a person's expectation of privacy is not contravened when his or her movements on a public highway are monitored with the assistance of a beeper, even where the device has been placed in a container being transported on or in a vehicle. The Court held that there is no reasonable expectation of privacy which accompanies a traveler on a public road; therefore, one cannot reasonably expect that his or her movements will not be scrutinized when they are exposed to public view.[125]

---

[122]DoD 5240.1-R, Procedure 5, Part 2, § F.1. See supra table 4-1.

[123]DoD 5240.1-R, Procedure 6, § B.3.

[124]DoD 5240.1-R, Procedure 6, § B.3.

[125]United States v. Knotts, 460 U.S. 276 (1983). In Knotts, the Supreme Court held that monitoring the signal of a beeper placed in a container of chemicals that was being transported to the owner's cabin did not invade any legitimate expectation of privacy on the cabin owner's part and, therefore, there was neither a "search" nor a "seizure" within the contemplation of the Fourth Amendment.

c. In such circumstances, the monitoring of signals and the locating of the "beeperized" object would constitute "concealed monitoring" under Procedure 6. However, as soon as this monitoring activity crosses the threshold into the person's zone of protected privacy, such as entry of a "beeperized" automobile into a private garage, monitoring of the beeper brings Fourth amendment rights into play.[126] The activity then becomes "electronic surveillance" and requires treatment and approval under DoD 5240.1-R, Procedure 5.

5-8. CONCEALED MONITORING OR ELECTRONIC SURVEILLANCE?

a. In the specific example cited above, the law requires one of two approaches. First, if the activity is treated as concealed monitoring, the beeper must be "turned off" upon entry of the "beeperized" car into the zone of protected privacy. The alternative is prior approval or authorization (e.g., a warrant under the Foreign Intelligence Surveillance Act) for the entire operation as electronic surveillance.

b. The presence or absence of this reasonable expectation of privacy is the most fundamental distinction between "concealed monitoring" and "electronic surveillance."

NO REASONABLE EXPECTATION OF PRIVACY = CONCEALED MONITORING

REASONABLE EXPECTATION OF PRIVACY = ELECTRONIC SURVEILLANCE

c. While this may be somewhat of an over-generalization, it is true most of the time, at least where electronic devices are involved.

5-9. THE WARRANT REQUIREMENT. Finally, in order for an activity to come within the coverage of Procedure 6 as concealed monitoring, the circumstances must be such that no warrant would be required if undertaken for law enforcement purposes.[127] This requirement is merely an extension of the "reasonable expectation of privacy" factor. Where such expectation exists, a warrant will be required, and where the investigative technique employed contemplates the use of some sort of electronic device, the result will NOT be concealed

---

[126]See e.g. United States v. Karo, 468 U.S. 705 (1984). In Karo, the Supreme Court held that (i) government is not completely free to determine by means of an electronic device, without warrant and without probable cause or reasonable suspicion, whether a particular article or person is in an individual's home at a particular time; and (ii) government is not free to do so without a warrant even if there is requisite justification in facts for believing that a crime is being or will be committed and that monitoring a beeper wherever it goes is likely to produce evidence of criminal activity.

[127]DoD 5240.1-R, Procedure 6, § A.1.

monitoring. It will be electronic surveillance, and must be handled in accordance with DoD 5240.1-R, Procedure 5.

5-10. ESSENTIAL ELEMENTS OF CONCEALED MONITORING.

a. In addition to meeting the scope tests discussed above, concealed monitoring is comprised of five essential elements. All five elements must be present for the object activity to be properly characterized as concealed monitoring. Those essential elements are --

(1) targeting

(2) by electronic, optical, or mechanical devices

(3) a particular person or group of persons

(4) without their consent

(5) in a surreptitious and continuous manner[128]

b. Targeting means that the monitoring is being specifically directed against a particular person or group of persons. And for the activity to be categorized as concealed monitoring, it must be done by electronic, optical, or mechanical devices. Now, this does not mean that DoD intelligence activities are permitted to indiscriminately use electronic, optical, or mechanical devices, so long as they are not directed against a person or group of persons. We do not have a lawful function or mission to conduct "indiscriminate monitoring." However, it does mean that where a legitimate function exists to monitor a particular place, while not "targeting" a person or group of persons, then such monitoring may be conducted outside the purview of Procedure 6.[129]

c. For example, if during the course of a bona fide counterintelligence operation it is necessary to conduct optical surveillance of a building entrance, such a surveillance would not be subject to the conditions of Procedure 6, so long as the target of that monitoring is not a particular person or group of persons. There are, of course, other boundaries to the conduct of such activity. But, where a legitimate mission or function exists to monitor public places and not people, then such monitoring is not within the purview of Procedure 6.

---

[128]DoD 5240.1-R, Procedure 6, § B.1.

[129]In some cases this activity could constitute physical surveillance where there is an intent to acquire information about a particular person. See DoD 5240.1-R, procedure 9, § B and infra chapter 6, § III.

d. The other three essential elements of concealed monitoring are fairly simple. Electronic, optical and mechanical devices includes the throng of modern high-tech items. 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. What constitutes a substantial period of time depends on the circumstances of the case involved. When in doubt, it is essential to secure the advice of your staff judge advocate or legal advisor.

5-11. LIMITATIONS AND RESTRICTIONS ON CONCEALED MONITORING. Limitations and restrictions pertaining to the use of concealed monitoring by DoD intelligence components are reflected in table 5-1. In all cases, requests for approval of concealed monitoring must be coordinated with the legal advisor to the approving authority.[130]

[130]DoD 5240.1-R, Procedure 6, § C.3.a.

Table 5-1
Concealed monitoring, DoD 5240.1-R, Procedure 6

GENERAL RULE: Concealed monitoring may be conducted by DoD intelligence components within the United States, or outside the United States against US persons, only for foreign intelligence (FI) and counterintelligence (CI) purposes, and only after approval. 1/

	PROCEDURES AND LIMITATIONS	
1.	Limitation on purposes	For FI and CI purposes only. 2/
2.	Restrictions within the United States	1. Conduct only at DoD leased or owned facilities; or 2. As part of an authorized CI investigation of -- a. Active US military personnel; b. Active duty actions of retired military personnel, active or inactive reservists or National Guard personnel; c. Present or former DoD contractor employees, after FBI waives jurisdiction; or 3. To assist the FBI in support of an FBI CI investigation in which the Army has interest. 3/
3.	Restrictions outside the United States	1. Conduct only at DoD leased or owned facilities; or 2. [redacted]
4.	Approval standards	1. Subject has no reasonable expectation of privacy. 2. Monitoring must be necessary to the conduct of an assigned FI or CI function. 3. Monitoring activity must not constitute electronic surveillance.
5.	DoD approval authorities 4/	1. Director, DIA 2. ASD/C3I

(b)(3):10 USC 424,(b)(3):50 USC 3024(i)

Table 5-1
Concealed monitoring, DoD 5240.1-R, Procedure 6

NOTES:

1/ The restrictions and limitations contained in Procedure 6 do not apply to concealed monitoring of non-US persons outside the United States. Such monitoring may be conducted in accordance with standards pertaining to approved operational missions in support of any lawful function assigned to a DoD intelligence component. However, concealed monitoring for foreign intelligence and counterintelligence purposes of a non-US person abroad, who has a reasonable expectation of privacy, will be treated as electronic surveillance. Such monitoring (i.e., electronic surveillance) is then subject to the limitations and restrictions contained in DoD 5240.1-R.

In addition, Procedure 6 does not affect other lawful concealed monitoring conducted in conjunction with the law enforcement responsibility of commanders, military police, criminal investigators, or security personnel, nor does it apply to actions by commanders pursuant to their responsibilities to maintain order and discipline within their military organizations. See, for example, AR 190-53, chapter 3, for procedures governing the use of pen registers and similar devices or techniques on military installations and targeted against persons subject to the Uniform Code of Military Justice.

2/ Counterintelligence includes efforts to protect against international terrorist activities, and does not include activities of personnel, physical, document or communications security programs.

3/ These include FBI counterintelligence investigations of DoD civilian personnel, US military personnel on active duty, retired military personnel, active and inactive reservists and National Guard members, and private contractors of the DoD and their employees. See "The Agreement Between the Deputy Secretary of Defense and the Attorney General, April 5, 1979," DoD 5210.84, "Security of DoD Personnel at U.S. Missions Abroad," and Appendix B of this handbook.

4/ In addition to the listed DoD approval authorities, concealed monitoring under Procedure 6 may also be approved by the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Director, National Security Agency; the Director, Naval Intelligence; the Director of Intelligence, US Marine Corps; the Assistant Chief of Staff, Intelligence, US Air Force; the Director, Naval Investigative Services; and the Commanding Officer, US Air Force Office of Special Investigations.

Section III

Procedure 7 - Physical Searches

5-12. SCOPE OF PROCEDURE 7. "Physical searches" are the subject of DoD 5240.1-R, Procedure 7. The scope of Procedure 7 extends to--

> ...unconsented physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes.[131]

5-13. SOME PERMISSIBLE ACTIVITIES.

a. In all cases where it is possible to obtain approval prior to conducting a physical search it must be secured. However, where a lawful arrest is made in circumstances which do not require securing a warrant, then the arresting DoD intelligence personnel may search the person arrested, and all areas in plain view. There are, of course, only limited situations in which DoD intelligence personnel are permitted to make lawful arrests, and those situations vary with the organization concerned. The arrest authority is a direct outgrowth of the mission assigned to the unit involved.[132]

c. Furthermore, where, as part of legitimate functions assigned to an DoD intelligence component, there is a reasonable suspicion that a person subject to that component's jurisdiction may be concealing weapons or contraband, then the person may be stopped and a pat-down conducted of his/her body for such weapons or contraband. If during the course of that pat-down objects are detected which could reasonably be the suspected weapons or contraband, those objects may be examined. And where weapons or contraband are found, there then exists a basis for an arrest, and the person may be fully searched incident to that lawful arrest.

5-14. OTHER MATTERS OUTSIDE THE SCOPE OF PROCEDURE 7.

a. Similarly, DoD intelligence component personnel may conduct a plain view examination of any physical space within their jurisdiction. And any contraband noted during that examination may be seized. In addition, DoD intelligence component commanders of installations and activities have the authority under the Manual for Courts-Martial, 1984 (MCM), Military Rules of Evidence (MRE), Rule 313, to inspect the physical spaces under their jurisdiction.

---

[131]DoD 5240.1-R, Procedure 7, § A.

[132]See, for example, AR 381-20.

These inspections could include the search of automobiles, briefcases, packages, and other items entering or leaving areas under the particular commander's control.

b. Commanders, including DoD intelligence component commanders, also have the authority under MCM, MRE, Rule 315, to authorize probable-cause searches of persons and places under their control in the exercise of their law enforcement responsibilities. The provisions of Procedure 7 are not intended to impinge upon the authority to conduct searches and inspections pursuant to these foregoing circumstances. However, DoD intelligence personnel need to use caution when using the "Commander Authorized Search". They must insure that the authorizing person is a true commander, designated as such on orders and one who exercises traditional military command authority. An "OIC", "Director", "Division Chief", etc. are generally NOT commanders for the approval of U.C.M.J. Commander Authorized Searches.

c. There is one additional point about the scope of Procedure 7. DoD intelligence components may be assigned to provide assistance to the FBI and other law enforcement authorities in conducting physical searches in accordance with DoD 5240.1-R, Procedure 12.[133] Within the United States, assistance to state and local law enforcement authorities is confined to circumstances where lives are endangered, and in all cases approval must be secured by an official listed in DoD 5240.1-R, following coordination with the appropriate DoD intelligence component General Counsel.

d. Assistance may also be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policies and applicable Status of Forces Agreements. DoD intelligence components, however, may not request or participate in activities against US persons that would not be otherwise permitted under Procedure 7, or any other provisions of DoD 5240.1-R.[134]

5-15. WHAT CONSTITUTES A PHYSICAL SEARCH? Within the context of DoD 5240.1-R, Procedure 7, a physical search means an unconsented intrusion upon a person or a person's property or possessions to obtain items of property or information. A physical search need not involve an actual physical penetration of a person's property.[135] An unconsented optical intrusion into space where one has a reasonable expectation of privacy would be a physical search within the meaning of Procedure 7.

---

[133]See infra chapter 8, § II, and Appendix B.

[134]DoD 5240.1-R, Procedure 12, § B.2.e.

[135]DoD 5240.1-R, Procedure 7, § B.

5-16. IMPLIED CONSENT. Procedure 7 does not control consensual searches. Consent to a physical search may be oral, or written, or implied from certain circumstances. 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, or what constitutes implied consent, should be referred to your supporting staff judge advocate or legal advisor.[136]

5-17. PLAIN VIEW EXAMINATIONS.

a. Procedure 7 also does not cover examinations of areas that are in plain view and visible to the unaided eye without physical trespass.[137] These so-called plain view spaces are not protected because persons in those places are not considered to have a reasonable expectation of privacy regarding their presence in such plain view. The use of various devices to aid the eye in viewing a particular space is an area of the law which is still in a state of development.[138] As technology advances, courts must address the use of new technologies by law enforcement and intelligence agencies. It is essential to keep in mind that the real issue in employing such devices is not whether the mere use of a particular device as sensory enhancement constitutes a generic search, but whether the purpose and use of a device invades legitimate expectations of privacy.

b. Because of the developing nature of the law in this area, it is essential to secure advice from your supporting staff judge advocate or legal advisor in any case where you are unsure regarding a persons reasonable expectation of privacy vis-a-vis an enhancement device planned for use in a particular area.

5-18. ABANDONED PROPERTY. Procedure 7 also does not cover examinations of abandoned property left in a public place, and does not reach to include any intrusion authorized as necessary to

---

[136]DoD 5240.1-R, Appendix A, ¶ 4.

[137]DoD 5240.1-R, Procedure 7, § B.

[138]For example, in United States v. Ishmael, 48 F. 3d 850, reh'g denied, United States v. Ishmael, 1995 U.S. App. LEXIS 11216 (5th Cir. Tex. Apr. 19, 1995), the Court of Appeals for the Fifth Circuit reversed a motion to suppress which had been granted by the U.S. District Court concerning the use of readings from a thermal imager in obtaining a search warrant. Citing Dow Chemical Company v. United States, 476 U.S. 227 (1986), the Court of Appeals stated that use of the thermal imager did not reveal "intimate details" of the defendant's activity and as such, its use was not precluded by the Fourth Amendment.

accomplish lawful electronic surveillance conducted pursuant to DoD 5240.1-R, Procedure 5, parts 1 and 2.[139]

5-19. UNCONSENTED PHYSICAL SEARCHES IN THE UNITED STATES.

a. Under Procedure 7, the jurisdictional authority of counterintelligence elements of the military departments to conduct unconsented physical searches within the United States is limited by the purpose of the proposed search and the status of the subject. Searches may be conducted only for counterintelligence purposes, and only of the person or property of active duty military personnel. Furthermore, absent exigent circumstances, the search must be authorized by a military commander empowered to approve such searches under the MCM, MRE, Rule 315(d). In all cases there must be a finding of probable cause to believe that the subject of the search is acting as an agent of a foreign power.[140] See table 5-2 for the criteria for determining that person is an "agent of a foreign power" for Procedure 7 purposes.

b. In all other circumstances, DoD intelligence components within the United States are prohibited from conducting physical searches for foreign intelligence and counterintelligence purposes. Requests, of course, may be made of the FBI to conduct such searches where necessary.[141] The procedures and standards necessary to support such requests are contained in table 5-2.

5-20. UNCONSENTED PHYSICAL SEARCHES OUTSIDE THE UNITED STATES.

a. Unconsented physical searches by DoD intelligence components of active duty military personnel outside the United States are subject to restrictions similar to those applicable within the United States (i.e., they are confined to counterintelligence purposes). Unless exigent circumstances exist, the searches must be approved by a military commander under the MCM, MRE, Rule 315. There must also be a probable cause finding that the subject is acting as an agent of a foreign power.

b. Unconsented physical searches of other US persons outside the United States are subject to the same restrictions as active duty military personnel with the additional requirement that approval must be obtained from the Attorney General of the United States.[142] The procedures and standards for securing these approvals are contained in table 5-2.

---

[139]DoD 5240.1-R, Procedure 7, § B.

[140]DoD 5240.1-R, Procedure 7, § C.1.a.

[141]DoD 5240.1-R, Procedure 7, § C.1.b.

[142]DoD 5240.1-R, Procedure 7, § C.2.

Table 5-2
Physical searches, DoD 5240.1-R, Procedure 7

GENERAL RULE: Unconsented physical searches of persons or property may be conducted by DoD intelligence components for foreign intelligence or counterintelligence purposes, but only after approval by a properly designated approval authority. 1/

LIMITATIONS AND RESTRICTIONS		
1. Limitations on purpose	Restricted to foreign intelligence and counterintelligence purposes	
2. Limitations on persons and property	1. Within the US -- restricted to persons and property of active duty military personnel 2/ 2. Outside the US --restricted to persons and property of US persons	

APPROVAL AUTHORITIES AND STANDARDS		
PERSON OR PROPERTY TO BE SEARCHED	AUTHORITIES	STANDARDS
1. Active duty military personnel 3/	Military Commander	Probable cause that the person is an agent of a foreign power 5/
2. Other US persons outside the US	Attorney General 4/	
3. Other US persons within the US	Not authorized 6/	Not applicable

Table 5-2
Physical searches, DoD 5240.1-R, Procedure 7

NOTES:

1/ Procedure 7 does not apply to consensual physical searches and does not affect any other lawful physical searches, or similar activities conducted in conjunction with the law enforcement responsibilities of commanders, military police, criminal investigators, or security personnel, and it does not apply to actions by a commander pursuant to his or her responsibilities to maintain order and discipline.

2/ DoD intelligence components may, however, request the FBI to conduct searches of other personnel for both foreign intelligence and counterintelligence purposes. When assistance is requested from the FBI, a copy of the request must be furnished to the DoD General Counsel.

3/ The military commander in these cases must be empowered to approve physical searches for law enforcement purposes pursuant to the Manual for Courts-Martial, Military Rules of Evidence, Rule 315(d).

4/ Requests for approval of unconsented physical searches of other US persons outside the US must be made by:
(1) The Secretary or the Deputy Secretary of Defense;
(2) The Secretary or the Under Secretary of a Military Department;
(3) The Director, National Security Agency; or
(4) The Director, Defense Intelligence Agency.

5/ a. For the purposes of Procedure 7, the term "agent of a foreign power" means that there is probable cause to believe that the subject of the search is:

(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 who conspires with, or knowingly aids and abets a person engaging in such activities;

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

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

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

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

Table 5-2
Physical searches, DoD 5240.1-R, Procedure 7

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

b. Requests for approval or authorization of these probable-cause searches must include the following information:

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

(2) A statement of facts supporting a finding that there is probable cause to believe the subject of the search is an agent of a foreign power, as defined above.

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

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

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

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

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

6/ The FBI should be requested to conduct such searches. See Note 2/ above.

Section IV

Conclusion to Chapter 5

5-21. PRESIDENTIAL GOALS. Part 1 of Executive Order 12333, United States Intelligence Activities, which was issued by President Reagan on 4 December 1981, states in part --

> All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council.[143]
>
> * * *
>
> Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence against the United States Government, or United States corporations, establishments, or persons.[144]

5-22. BALANCING COMPETING INTERESTS.

a. These goals of the President concurrently reflect the significance of the United States intelligence community in the preservation of our free society, and the delicate balancing of competing interests that we pursue on a constant basis. It is important that we always keep these competing interests in perspective. Intelligence does not exist for the sake of itself, and the Department of Defense does not exist to perpetuate itself. Both are instruments of the Executive and of the people of the United States, and would not exist were it not for the will of the citizenry and the perceived need to protect our institutions and way of life.

b. In carrying out our mission and functions, we must view the legal and regulatory framework within which we operate as our route to success, and not as roadblocks to progress. Our success is not measured solely by what we achieve, but by the degree of our achievement while preserving our cherished values. Certainly, our adversaries may be markedly more successful in the quantity of their information acquisitions through concealed monitoring, physical searches, and the unbridled use of other collection techniques. But their quantity of success will always be inversely proportionate to their quality of life.

---

[143] E.O. 12333, Pt. 1.1(b).

[144] E.O. 12333, Pt. 1.1(c).

Chapter 6

MAIL SURVEILLANCE AND PHYSICAL SURVEILLANCE

Section I

Introduction

6-1. GENERAL. The rules for DoD 5240.1-R, Procedure 8 (Searches and Examination of Mail) and 9 (Physical Surveillance), both of which are "special collection techniques"[145] within the meaning of DoD 5240.1-R, are covered in this chapter.

6-2. USE OF MAIL SURVEILLANCE.

a. The use of all special collection techniques by DoD intelligence components, including mail searches and covers, must be based upon a determination that the selection of one of those techniques amounts to the employment of the least intrusive investigative technique reasonably available to collect the required information.[146]

b. Applicable postal regulations do not permit DoD intelligence components to detain or open first class mail within the United States postal channels for foreign intelligence or counterintelligence purposes, or to request such action by the postal service.[147] Intelligence components may, however, request assistance from the FBI where applicable, and may initiate mail covers for foreign intelligence and counterintelligence purposes, and mail searches for law enforcement purposes.

6-3. USE OF PHYSICAL SURVEILLANCE. The use of physical surveillance is subject to the same rules as other special collection techniques. Within the United States, however, for the purposes of determining whether additional limitations apply to use of physical surveillance in the collection of foreign intelligence, a distinction must be made between overt and covert physical surveillance.

a. Where physical surveillance is carried out in a covert manner (i.e., concealed from notice, but not necessarily from view), coordination must be effected with the FBI and there must be a determination by the head of the intelligence component concerned, or his or her single designee, that the use of other than overt means is reasonably necessary to accomplish the mission.

---

[145]See supra chapter 3, § III.

[146]DoD 5240.1-R, Procedure 2, § D.2.

[147]DoD 5240.1-R, Procedure 8, § C.1.a.

Section II

Procedure 8 - Searches and Examination of Mail

6-4. SCOPE OF PROCEDURE 8.

a. DoD 5240.1-R, Procedure 8, is fairly simple in its scope - it applies to all mail opening and mail covers in United States postal channels for foreign intelligence and counterintelligence purposes. In general, the following is required:

(1) Mail covers will be requested and used within the United States in accordance with postal service regulations;[148] and outside the United States in accordance with the law of the host country;[149]

(2) Opening mail sealed against inspection (i.e., first class mail) in United States postal channels, including APO and FPO channels, is permitted only in accordance with a judicial warrant or search authorization issued pursuant to law;[150]

(3) Opening mail to or from US persons found outside United States postal channels, including APO and FPO channels, is permitted only with the approval of the Attorney General of the United States.[151]

b. With these three general rules in mind, an explanation of the terms used in Procedure 8 seems appropriate. As you have already seen, many of the terms and words used in DoD 5240.1-R have peculiar meanings within the context of intelligence activities. Often, the plain meaning of a word or term is not the meaning ascribed in DoD 5240.1-R. Procedure 8 is no different.

6-5. SEARCHES OF MAIL.

a. The term "searches of mail" is not specifically defined in DoD 5240.1-R; however, the term "opening of mail" is used repeatedly as a synonym. For the purposes of Procedure 8, that - opening of mail - is precisely what constitutes the searches of mail. Mail, since as far back as 1878, has been considered by the Supreme

---

[148]DoD 5240.1-R, Procedure 8, § C.3.a. These regulations include the DoD Postal Manual, DoD 4525.6-M and the US Postal Service rules and regulations, 39 C.F.R. Part 233.

[149]DoD 5240.1-R, Procedure 8, § C.3.b.

[150]DoD 4525.6-M, chapter 8, § I, and 39 C.F.R. § 233.3.

[151]See DoD 5240.1-R, Procedure 8, § C.2.a. These approval requests shall be treated as a request for an unconsented physical search under Procedure 7, § C.2.b.

Court of the United States as being protected against opening and inspection, except in accordance with the Fourth Amendment to the Constitution.[152] - and the Fourth Amendment protects against unreasonable searches and seizures - hence we see that opening mail is a search for Fourth Amendment purposes.

b. In 1878, the Supreme Court of the United States recognized that the postal powers of the Congress[153] embrace all measures necessary to ensure the safe and speedy transit and prompt delivery of the mails.[154] And not only are the mails under the protection of the National Government, they are in contemplation of the law its property.[155] This theory has caused some consternation over the years for the Congress and the courts.

c. For example, Congress, in a provision in the Postal Services and Federal Employees Salary Act of 1962,[156] authorized the Post Office Department to detain material determined to be "communist political propaganda" and forward it to the addressee only if requested after notification by the Department. The apparent reasoning leading to this statute was that if mails are in the contemplation of the law the Government's property, then the Government has a right to regulate anti-government content of its own property.

---

[152]Ex parte Jackson, 96 U.S. 727 (1878); United States v. van Leeuwen, 397 U.S. 249 (1970). The Court has had somewhat more difficulty dealing with application of the First Amendment to the mails. In 1872, Congress passed the first of a series of acts to exclude from the mails publications designed to defraud the public or corrupt its morals. In Ex parte Jackson, the Court sustained the exclusion of lottery circulars from the mails stating that "the right to designate what shall be carried necessarily involves the right to determine what shall be excluded." 90 U.S. 732. Nearly half a century later, the Court sustained an order of the Postmaster General excluding from the mails published material found in contravention of the Espionage Act of 1917. United States ex rel. Milwaukee Publishing Co. v. Burleson, 255 U.S. 407 (1921). Finally, 44 years later, a unanimous Court struck down a statute authorizing the Post Office to detain mail it determined to be "communist political propaganda." Lamont v. Postmaster General, 381 U.S. 301 (1965). In this, the first congressional statute ever voided as in conflict with the First Amendment, the Court said: "The United States may give up the Post Office when it sees fit, but while it carries it on the use of the mails is almost as much a part of free speech as the right to use our tongues..." Id., 305, quoting Justice Holmes in United States ex rel. Milwaukee Publishing Co. v. Burleson, 255 U.S. 407, 437 (1921) (dissenting opinion).

[153]U.S. Const. art. 1, § 8, cl. 7.

[154]Ex parte Jackson, 96 U.S. 727, 732 (1878).

[155]Searight v. Stokes, 3 How. (44 U.S.) 151 (1845). This principle was recognized by the Supreme Court in holding that wagons carrying United States mail were not subject to a state toll tax imposed for use of the Cumberland Road pursuant to a compact with the United States.

[156]Act of October 11, 1962 (§ 305, 76 Stat, 840).

d. A mere three years after passage, the law was struck down by the Supreme Court as an unconstitutional abridgment of the First Amendment rights. The Court said that although Congress was not bound to operate a postal service, while it did, it was bound to observe constitutional guarantees.[157] This, of course, applies to the Fourth Amendment guarantee against unreasonable searches and seizures, as well as the First Amendment guarantees of freedom of religion and expression.

6-6. EXAMINATION OF MAIL. To examine mail means to employ a mail cover on such mail. 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.[158] It also includes checking the contents of any second, third, or fourth class mail in order to obtain information in the interest of protecting national security, locating a fugitive, or obtaining evidence of commission or attempted commission of a crime.[159]

6-7. MAIL WITHIN UNITED STATES POSTAL CHANNELS.

a. Mail is considered to be within US postal channels until the moment it is delivered manually in the United States to the specific addressee named on the envelope, or an authorized agent. In addition, for the purposes of DoD 5240.1-R, Procedure 8, mail is considered to be within US postal channels when any one of the following conditions exist:

(1) In transit within, among, and between the United States, its territories and possessions, and Army-Air Force (APO) and Navy (FPO) post offices;

(2) Mail of foreign origin which has passed by a foreign postal administration to the US Postal Service for forwarding to a foreign postal administration under a postal treaty or convention;

(3) Mail temporarily in the hands of the US Customs Service or the Department of Agriculture;

(4) International mail enroute to an addressee in the United States or its possessions after passage to the US Postal Service from a foreign postal administration or enroute to an addressee abroad before passage to a foreign postal administration; or

---

[157]Lamont v. Postmaster General, 381 U.S. 301 (1965).

[158]DoD 5240.1-R, Procedure 8, § B.3.

[159]DoD 4524.6-M, Chapter 8, § I.8.a(3).

(5) Mail for delivery to the United Nations in New York City.[160]

b. A letter, package, or other item becomes "mail" for our purposes as soon as it enters the US Postal Service system, and it retains its character as "mail" until it leaves that system, either by delivery to the intended addressee or to the addressee's agent.[161]

6-8. CLASSES OF MAIL.

a. Mail is divided into four classes. Intelligence components are prohibited from detaining or opening first class mail within US postal channels for foreign intelligence or counterintelligence purposes, and from even requesting such action by the US Postal Service. For postal regulation purposes, first class mail is considered sealed against inspection, and searches and seizures of first class mail in US postal channels may be authorized only upon probable cause and an appropriate warrant.

b. Second, third, and fourth class mail is termed not sealed against inspection, and may be detained, inspected or opened in a variety of legitimate circumstances by postal officials, including pursuant to an approved DoD intelligence component mail cover.[162]

6-9. MILITARY POSTAL SYSTEM OVERSEAS. The DoD Postal Manual, DoD 4525.6-M, provides that military commanders, including MI commanders, exercising special court-martial jurisdiction, and military judges have the authority under the Manual for Courts-Martial (MCM), Military Rules of Evidence (MRE), Rule 315, to authorize probable-cause searches and seizures of all four classes of mail when such search or seizure is to occur within the Military Postal System overseas, although such an order is not required for second, third, or fourth class mail.[163]

6-10. JUDICIAL WARRANTS. Judicial warrants to search first class mail in other portions of the US postal system must be secured in Federal judicial proceedings pursuant to the Federal Rules of Criminal Procedure, Rule 41.[164]

---

[160]DoD 5240.1-R, Procedure 8, § B.1.b.

[161]DoD 5240.1-R, Procedure 8, § B.1.b

[162]39 C.F.R. § 233.3(f).

[163]DoD 4525.6-M, Chapter 8, §§ I.3 and I.6.

[164]See 39 C.F.R. § 233.3(g) and DoD 4525.6-M, Chapter 8, § I.6.

6-11. APPROVAL FOR MAIL COVERS.

a. Mail covers, on the other hand, may be conducted pursuant to an order issued by an appropriate postal official, based upon a written request from a law enforcement agency. This request will contain a stipulation by the requesting authority that specifies the reasonable grounds that exist which demonstrate that the mail cover is necessary to protect the national security, locate a fugitive, or obtain information regarding the commission or attempted commission of a crime. For the purposes of seeking mail covers, the counterintelligence elements of DoD intelligence components are considered law enforcement agencies, but their jurisdiction is limited to counterintelligence matters with criminal law implications, such as espionage, sabotage, and international terrorism.[165]

b. DoD 4525.6-M provides that within the Military Postal System overseas, the senior military official who has responsibility for postal operations of each major command within each military service may order mail covers within the geographic area of the major overseas commands to which they are assigned. Limited delegation of this authority is authorized; however, delegation is not permitted to approve national security requests. DoD intelligence personnel must become familiar with the procedures and authorities within their respective overseas geographic commands.[166]

c. For other elements within the US Postal Service system, mail covers may be ordered pursuant to the authority of the Chief Postal Inspector of the Postal Service, and according to procedures and standards specified in 39 C.F.R. Part 233.3.[167]

d. DoD intelligence components may request mail covers within US postal channels only for counterintelligence purposes.[168] According to postal regulations, this means to protect national security. Postal regulations state that "protect national security" means to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents:

---

[165]39 C.F.R. Part 233.3(f).

[166]DoD 4525.6-M, Chapter 8, § I.8.b.

[167]The United States Postal Service maintains rigid controls and supervision over the use of mail covers. Mail covers may be ordered to obtain information in the interest of protecting the national security, locating a fugitive, or obtaining evidence of commission or attempted commission of a crime. Authorization may be issued by The Chief Postal Inspector or a Postal-Inspector-In-Charge for up to 120 days.

[168]DoD 5240.1-R, Procedure 8, § C.3.a.

(1) An attack or other grave hostile act;

(2) Sabotage, or international terrorism; or

(3) Clandestine intelligence activities.[169]

6-12. EMERGENCY SITUATIONS. Finally, within US postal channels, any military postal clerk or postal officer or any person acting under the authorization of such a clerk or officer may detain, open, remove from postal custody, and process or treat mail, of any class, reasonably suspected of posing an immediate danger to life or limb, or an immediate and substantial danger to property, without a search warrant or authorization. This detention, however, is limited to the extent necessary to determine and eliminate the danger, and a complete written report along with details must be filed promptly after the incident.[170]

6-13. MAIL OUTSIDE UNITED STATES POSTAL CHANNELS.

a. Outside US postal channels, there is a two-tier approach to mail searches by DoD intelligence components.

(1) First, if the search is to involve mail to or from a US person, it must be authorized by the Attorney General of the United States, and treated as an unconsented physical search under DoD 5240.1-R, Procedure 7, § C.2.b.[171] That means that there must be a probable cause to believe that the subject of the search is acting as an agent for a foreign power. See table 6-1.

(2) Second, when both the sender and intended recipient are non-US persons, heads of DoD intelligence components may authorize a search if such a search is otherwise lawful and consistent with applicable Status of Forces Agreements.

b. DoD intelligence components may also request mail cover of mail to or from a US person which is outside US postal channels in accordance with the appropriate law and procedure of the host government and any Status of Forces Agreement that may be in effect.[172]

---

[169]39 C.F.R. Part 233.3(c)(5).

[170]DoD 4525.6-R, Chapter 8, § I.4.

[171]DoD 5240.1-R, Procedure 8, § C.2.a.

[172]DoD 5240.1-R, Procedure 8, § C.3.b.

Table 6-1
Searches and examination of mail, DoD 5240.1-R, Procedure 8

GENERAL RULE: Searches of mail and mail covers may be conducted by DoD intelligence components only upon approval by a properly designated approval authority, and for counter intelligence purposes. 1/

	REGULATED ACTIVITY	AUTHORITIES	STANDARDS
1.	Search of first class mail within non-military portions of US postal channels	Federal Judge or magistrate 2/	Limited to law enforcement purposes - for DoD intelligence components means probable cause must exist to believe the person is an agent of a foreign power 4/
2.	Search of first class mail in overseas Military Postal Service part of US postal channels 3/	Military judge or SPCM Commander	
3.	Search of mail to or from US person found outside US postal channels 5/	Attorney General	
4.	Search of mail outside US postal channels when sender and recipient non-US persons 6/		Any lawful function assigned to a DoD intelligence component
5.	Request for mail cover outside US postal channels 7/		
6.	Requests to US postal officials to conduct mail cover in US postal channels, including the overseas military postal system		Counterintelligence or national security purposes only 8/
7.	Requests to US postal authorities to detain or permit detention of other than first class mail that may become subject to search.	Any operational commander9/	Reasonable suspicion that person is an agent of a foreign power. 10/

Table 6-1
Searches and examination of mail, DoD 5240.1-R, Procedure 8

NOTES:

1/ Procedure 8 does not apply to lawful searches of mails or mail covers conducted in conjunction with the law enforcement responsibilities of commanders, military police, criminal investigators, or security personnel, and it does not apply to actions by a commander pursuant to his or her responsibility to maintain order and discipline.

2/ DoD intelligence components are not permitted to detain or open first class mail within US postal channels for foreign intelligence or counterintelligence purposes, or to request such action by the US Postal Service. Searches of first class mail are permitted for law enforcement purposes. When a DoD intelligence component has a bona fide law enforcement justification to request search of first class mail within the non-Military Postal System portions of US postal channels, the matter must be either referred to the appropriate agency with jurisdiction (e.g., FBI for civilians within the United States), to secure a judicial warrant pursuant to the Federal Rules of Criminal Procedure, Rule 41. The only law enforcement basis to seek such a search warrant by DoD intelligence components is a probable cause showing that person under military jurisdiction is an agent of a foreign power.

3/ The military judge or commander in these cases must be empowered to approve searches for law enforcement purposes pursuant to the Manual for Courts-Martial, 1984, (MCM), Military Rules of Evidence (MRE), Rule 315(d). This includes --

a. A commanding officer authorized to convene a special court-martial under the Uniform Code of Military Justice, Article 23(a), who is authorized by the MCM to issue search authorizations for the particular individual or location involved, or

b. A military judge or magistrate authorized by Military Service regulations to issue search authorizations.

Table 6-1
Searches and examination of mail, DoD 5240.1-R, Procedure 8

4/ a. For the purposes of requesting mail searches, the term "agent of a foreign power" means that there is probable cause to believe that the subject of the search is:

(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;

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

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

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

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

Table 6-1
Searches and examination of mail, DoD 5240.1-R, Procedure 8

b. Requests for approval or authorization of these probable-cause mail searches must include the following information:

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

(2) A statement of facts supporting a finding that there is probable cause to believe the subject of the search is an agent of a foreign power, as defined above.

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

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

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

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

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

5/ Requests for Attorney General approval in these cases are to be treated as requests for unconsented physical search under DoD 5240.1-R, Procedure 7. The standards that apply for securing search authorizations and warrants are the same as those applicable to establishing a probable-cause that the person involved is an agent of a foreign power. (See table 5-2, note 5.)

Table 6-1
Searches and examination of mail, DoD 5240.1-R, Procedure 8

6/ In these cases, searches must also be lawful and consistent with any Status of Forces Agreement that may be in effect.

7/ These mail cover activities must be in accordance with the appropriate law and procedure of the host government and any Status of Forces Agreement that may be in effect.

8/ DoD intelligence components may only request mail covers within US postal channels for counterintelligence (i.e., national security) purposes. This includes, for DoD 5240.1-R purposes, information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorists activities, but does not include actual or potential threats to the security of the United States by a foreign power or its agents, from an attack or other grave hostile act; sabotage, or international terrorism; or clandestine intelligence activities.

9/ This authority includes any operational commander who has the authority to pursue investigative matters which could result in a request to secure a warrant or search authorization based on a probable cause showing that the person involved is an agent of a foreign power. The subject of the investigation must be someone under DoD intelligence investigative jurisdiction; otherwise, the case must be referred to the agency which holds such jurisdiction. Requests must also be coordinated with the legal advisor to the approving authority and information copies of such request must be provided as appropriate.

10/ DoD 4525.6-M permits a military postal clerk or postal officer to detain mail based upon reasonable suspicion, for a brief period of time not to exceed 72 hours, so that military officials acting diligently and without delay may assemble enough evidence to satisfy the probable cause requirement for a warrant or search authorization. A reasonable suspicion required is more than a mere "hunch". In one recent case, the Supreme Court laid out several principles to be applied in determining whether reasonable suspicion exists. The Court said, that considering the totality of the circumstances, there must be a "particularized and objective basis for suspecting the particular person...of criminal activity."

Section III

Procedure 9 - Physical Surveillance

6-14. SCOPE OF PROCEDURE 9. DoD 5240.1-R, Procedure 9, covers physical surveillance. This procedure applies only to the physical surveillance of US persons by intelligence components for foreign intelligence and counterintelligence purposes.

6-15. WHAT IS PHYSICAL SURVEILLANCE? The term "physical surveillance" should not be given a literal interpretation. There are two alternative definitions for the term, and each contains four essential elements. Unless a particular activity meets all the essential elements of one or the other definition, it is not "physical surveillance" within the ambit of Procedure 9. It is not even sufficient to meet three out of four elements in each alternative, or any other odd combination - its four in one, or nothing at all.[173]

a. Under one definition, call it Alternative No. 1, physical surveillance means --

(1) a systematic and deliberate observation

(2) of a person

(3) by any means

(4) on a continuing basis.

b. Under the other definition, call it Alternative No. 2, physical surveillance also means --

(1) the acquisition

(2) of a nonpublic communication

(3) by a person not a party thereto or visibly present thereat

(4) through any means, not involving electronic surveillance.

6-16. THE ESSENTIAL ELEMENTS.

a. Now that we are comfortably immersed in semantic hyperbole, perhaps a brief discussion of those individual elements in each alternative definition will be helpful to an understanding of Procedure 9.

---

[173]DoD 5240.1-R, Procedure 9, § B.

b. As mentioned earlier, a particular activity must meet all four essential elements of one alternative or the other to be classified as physical surveillance for the purposes of DoD 5240.1-R, Procedure 9. The precise meaning of most of those elements, eight altogether, is fairly obvious, so further extensive explanation is not really necessary. Others may be a little more elusive, and examples may help.

6-17. ESSENTIAL ELEMENTS OF ALTERNATIVE NO. 1. Alternative No. 1 in physical surveillance is a systematic and deliberate observation, of a person, by any means, on a continuing basis.

a. Systematic and deliberate means that the activity must be both methodical or done with purposeful regularity,[174] and intentional or premeditated.[175] Note that there are two parts to this element. They are coextensive in their application to Procedure 9. Both parts must be there to establish the presence of this element. For example, case officer Brodrick is assigned to conduct a physical surveillance of Ivan. The activity is planned and carried out - Brodrick waits outside Ivan's luncheon kiosk, and begins to follow Ivan on foot on Ivan's return to his office. The surveillance is systematic and deliberate. On the other hand, if Brodrick knows Ivan, and makes an appointment to have lunch with him at the kiosk, and then accompanies him back to his office after lunch - Brodrick is not conducting a physical surveillance. The latter activity may be designed to keep track of Ivan's activities, but inasmuch as Ivan consented to have Brodrick present, the "keeping track" does not constitute physical surveillance for the purposes of DoD 5240.1-R, Procedure 9.

b. A person, within the ambit of Alternative No. 1, means a natural person. Recall that the broader definition of a person for DoD 5240.1-R purposes includes non-natural entities, such as corporations, partnerships, associations.[176] But those are abstract entities, and the observation which is contemplated in physical surveillance is one which encompasses finite objects, not abstractions. So, if Brodrick is assigned the task of keeping track of ABC Corporation, it will not be possible for him to conduct a physical surveillance of the corporation, per se. It may be necessary to conduct a physical surveillance of some natural person affiliated with the corporation, and that must be treated as a physical surveillance. But that is separate activity from just keeping track of the corporation. Brodrick may also employ other special collection techniques, such as physical searches or mail covers, to keep track of ABC Corporation, in which case the rules

---

[174]The American Heritage Dictionary 1306 (New College Ed. 1976).

[175]The American Heritage Dictionary 349.

[176]See supra ¶ 3-9. DoD 5240.1-R, Appendix A, ¶ 27.

in Procedure 7 or 8 would apply. But the laws of physics would render the actual physical surveillance of the corporation impossible.

c. By any means is pretty self-explanatory, except that the use of some means may necessarily trigger other rules in this area of special collection techniques. For example, the occasional use of binoculars during a physical surveillance can reasonably be considered nothing more than an acceptable visual adjunct to that activity. On the other hand, augmentation of the surveillance effort by a beeper in a package or attached to a car would trigger the rules pertaining to concealed monitoring in Procedure 6.[177]

d. On a continuing basis means conducted without interruption for a substantial period of time. What constitutes a substantial period of time will depend on the circumstances of the case. Incidental observations made in the course of a surveillance are not included.

6-18. ESSENTIAL ELEMENTS OF ALTERNATIVE NO. 2. Alternative No. 2 defines physical surveillance as the acquisition of a nonpublic communication, by a person not a party thereto or visibly present thereat, through any means, not involving electronic surveillance.

a. Acquisition is self-explanatory. It is the first step in the collection process which is defined under DoD 5240.1-R, Procedure 2. Recall that for information to be collected for the purposes of DoD 5240.1-R, it must be both acquired and some affirmative action must be taken to demonstrate an intent to use or retain that information.[178] For the purposes of Procedure 9, Alternative No. 2, an "intent" to retain or disseminate the information product of the surveillance is unnecessary. The test is one of merely "acquiring the information."

b. What constitutes a nonpublic communication for Procedure 9 purposes is somewhat problematic. Under our discussions of other special collection techniques, such as electronic surveillance and physical searches, we have discussed at length the concept of a reasonable expectation of privacy. In fact, under Procedure 5, Electronic Surveillance, we considered the specific application of this concept to the acquisition of nonpublic communications by electronic surveillance.[179] Unfortunately, the definition of nonpublic communications for Procedure 9 purposes is not the same as the definition for Procedure 5, electronic surveillance purposes.

---

[177]See supra ¶¶ 4-17c, 5-7b and 5-7c.

[178]See supra ¶ 3-7.

[179]See supra ¶ 4-11b.

c. Let's examine that difference briefly. It's important to fully understand that where there is a reasonable expectation of privacy involved in any communication, the intrusion by government into that zone of privacy constitutes entry into a protected sphere.[180] Whatever rights the communicants have must be observed. For example, if the activity occurs against US persons in the United States, then the Fourth Amendment applies, and a judicial warrant or search authorization is required - regardless of the means employed in the acquisition. If electronic means are employed, then the activity is electronic surveillance. If only human means are employed, then any other unconsented intrusion necessary to penetrate the protected zone of privacy will necessarily constitute a physical search, thus triggering the warrant/authorization requirements of Procedure 7.[181] Therefore, if an activity truly contemplates acquisition of a communication in which the parties have a reasonable expectation of privacy that the contents of that communication will remain private, then it CANNOT be physical surveillance.

(1) Nonpublic communication, then, for Procedure 9, Alternative No. 2, purposes has nearly a generic meaning. To find this meaning we must first look at DoD 5240.1-R, Appendix A, which defines "available publicly" as follows:

> 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

---

[180]From a constitutional standpoint, however, where communications are concerned, a reasonable expectation of privacy must exist on the part of all communicants for the "sphere" to retain its protection from intrusion. If one communicant consents to governmental intrusion, then the Fourth Amendment rights of all communicants are effectively vitiated. See e.g., United States v. White, 401 U.S. 745 (1971) and Rathbun v. United States, 355 U.S. 107 (1957). In White, the Supreme Court held that where a radio transmitter had been concealed on the person of an informant with knowledge of the informant, and where conversations between the informant and defendant were overheard by government agents without a warrant, who testified as to the conversations at the defendant's trial, there was no violation of the defendant's Fourth Amendment right to be secure against unreasonable searches and seizures. In Rathbun, the Court held that contents of a communication overheard on a regularly used telephone extension by police officers, with consent of one of the parties to the conversation, was admissible in federal court. It should be noted that while both these examples involve circumstances where a warrant is not required, for DoD intelligence purposes they would be, depending on the specific facts, either "consensual electronic surveillance" (DoD 5240.1-R, Procedure 5, § C) or "concealed monitoring" (DoD 5240.1-R, Procedure 6, § B.1), and would require prior approval under DoD 5240.1-R.

[181]See supra ¶ 5-19.

even though the military community is not open to the civilian general public.[182]

(2) This would seem to suggest that the DoD 5240.1-R generic meaning of nonpublic communication would be communication that is neither available for general public consumption, nor lawfully available to the casual observer.

(3) Now, all this may seem too much like a discussion about how many angels can dance on the head of a pin, but the key to our analytical, constructive definition of nonpublic communication for Procedure 9 purposes seems to lie in that phrase: not lawfully available to the casual observer.

(4) If Brodrick sits down at the kiosk luncheon counter next to Ivan and listens casually to Ivan's conversation, he is not conducting physical surveillance because Ivan's conversation is available to any casual observer. On the other hand, if Brodrick knows that Ivan always uses the same booth at the kiosk, and Brodrick secrets himself in the hollow seat of the booth in order to hear the whispers of Ivan to Fidel during their luncheon meeting, then Brodrick is conducting physical surveillance. Furthermore, note that the conversation is taking place in a space open to the public. As such, it is not possible to say that Ivan and Fidel have a protected zone of privacy. The judicial warrant or search authorization protective procedures do not extend to these circumstances. Nevertheless, the regulatory oversight mechanism of the intelligence community system applies. Approval under Procedure 9 applies to this physical surveillance activity.

d. The last two elements in alternative no. 2, by a person not a party thereto or visibly present thereat and through any means, not involving electronic surveillance, have already been discussed or are self evident and require no further discussion.

6-19. PHYSICAL SURVEILLANCE AND CONCEALED MONITORING COMPARED.

a. It is useful to note, beyond some of our brief suggestions above, the very distinct similarity between physical surveillance and concealed monitoring under Procedure 7. The important differences between the two are that concealed monitoring always involves the use of some electronic, optical or mechanical device,[183] while physical surveillance need not involve such devices. Concealed monitoring must be surreptitious,[184] while physical surveillance may be done with the knowledge of a subject.

---

[182]DoD 5240.1-R, Appendix A, ¶ 2.

[183]DoD 5240.1-R, Procedure 6, § B.1.

[184]DoD 5240.1-R, Procedure 6, § B.1.

Both are nonconsensual, and there are some circumstances in which the techniques may overlap.

b. For example, recall from one of our earlier examples that observation of a subject during a street surveillance on foot, or following in an automobile, would be a simple example of physical surveillance.[185] However, if the surveillance is augmented with a beeper attached to the subject's car, it becomes concealed monitoring. Further, a stationary surveillance of the exterior of a persons quarters by "unaugmented" human observation would be physical surveillance. Change the circumstances by placing a surreptitious television camera so as to target that specific person entering and leaving the building and you have concealed monitoring.

6-20. PHYSICAL SURVEILLANCE WITHIN THE UNITED STATES.

a. DoD intelligence components may conduct unconsented physical surveillance of US persons in the United States only for foreign intelligence and counterintelligence purposes, and only against persons within the investigative jurisdiction of the component conducting the surveillance. These persons include the following:[186]

(1) Present or former employees of the DoD intelligence component concerned,

(2) Present or former contractors of that DoD intelligence component,

(3) Present or former employees of present or former contractors of that DoD intelligence component,

(4) Applicants for employment with the DoD intelligence component concerned, or with the contractors of that component, or

(5) Members of the military services.

b. In addition, any physical surveillance of US persons that occurs outside a DoD installation in the United States must be coordinated with the FBI and other law enforcement agencies, as may be appropriate.[187]

---

[185]Supra ¶ 6-17a.

[186]DoD 5240.1-R, Procedure 9, § C.1.

[187]DoD 5240.1-R, Procedure 9, § C.1.

6-21. PHYSICAL SURVEILLANCE OUTSIDE THE UNITED STATES.

a. Outside the United States, DoD intelligence components may conduct physical surveillance of the same US person-subjects as permitted within the United States. They may also conduct physical surveillance of other US persons in the course of lawful foreign intelligence and counterintelligence investigations, subject to the following conditions:[188]

(1) Such surveillance must be consistent with the laws and policy of the host government, and may not violate any Status of Forces Agreement that may be in effect; and

(2) Physical surveillance of a US person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot not be obtained by other means.

---

[188]DoD 5240.1-R, Procedure 9, § C.2.

Table 6-2
Physical surveillance, DoD 5240.1-R, Procedure 9

GENERAL RULE: Physical surveillance may be conducted by DoD intelligence components only upon US persons for foreign intelligence and counterintelligence purposes. 1/

REGULATED PHYSICAL SURVEILLANCE	AUTHORITIES	STANDARDS
1. Against US persons within investigative jurisdiction of the DoD in the United States 2/	1. Head of DoD intelligence component 2. Designated senior intelligence component officials	1. Limited to FI & CI purposes 2. Outside DoD installation must coordinate with the FBI 3/
2. Against US persons not within investigative jurisdiction of the DoD within the United States 4/	Not authorized 5/	Not applicable
3. Against US Persons within investigative jurisdiction of the DoD outside the United States	1. Head of DoD intelligence component 2. Designated senior intelligence component officials	1. Limited to FI & CI purposes
4. Against US persons not within investigative jurisdiction of the DoD outside the United States	Deputy Under Secretary of Defense (Policy) [redacted]	1. Limited to FI & CI purposes 2. Conform to host country laws and any SOFA 7/ 3. Must provide significant information not available by other means

(b)(3):10 USC 424,(b)(3):50 USC 3024(i)

NOTES:

1/ DoD 5240.1-R, Procedure 9, does not apply to consensual physical surveillance, such as that conducted as part of a training exercise where the subjects are participating in the exercise.

2/ US persons within DoD investigative jurisdiction, for purposes of Procedure 9, include US persons who are present or former employees of the component concerned; present or former contractors of such component or their present or former employees; applicants for such employment or contracting; or members of the military services.

Table 6-2
Physical surveillance, DoD 5240.1-R, Procedure 9

3/ Coordination must also be effected with any other law enforcement agency, as may be appropriate.

4/ DoD investigative jurisdiction is defined in "The Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979" and DoD 5210.84, "Security of DoD Personnel at U.S. Missions Abroad". This includes active duty US military personnel; active duty actions of retired military personnel, active or inactive reservists, or National Guard personnel; present or former DoD contractor employees, after FBI has waived jurisdiction; and assistance to the FBI in support of FBI counterintelligence investigations in which the DoD has an interest.

5/ The FBI should be requested to conduct this surveillance.

6/ See DoD 5240.1-R Procedure 9, § 3.b.

7/ "SOFA" means any Status of Forces Agreement which may be in effect.

Section IV

Conclusion

6-22. SUMMARY. "Special collection techniques" - electronic surveillance, concealed monitoring, physical searches, searches and examinations of mail, physical surveillance and undisclosed participation in organizations - are all so potentially intrusive that the policy announced by the President in E.O. 12333 mandates their use on only a limited basis.[189]

6-23. MISSION ACCOMPLISHMENT AND OVERSIGHT.

a. Each of us must be dedicated to mission accomplishment. But that dedication must encompass a full understanding of our DoD intelligence missions and functions, and goals and objectives. These missions, functions, goals and objectives all contain elements designed to provide oversight of our intelligence, counterintelligence and security activities. These elements of oversight, which include mandates to comply with rules and regulations, are inseparable from those missions, functions, goals and objectives. There is no place in our DoD intelligence activities that this concept is more important than in our considerations to employ those potentially intrusive techniques which are available to us. We must not be deterred from their legitimate use, but we must accept the fact that such use must explicitly be within the bounds of legality and ethical propriety.

b. The purpose of all regulatory procedures by which we must operate is to enable us to carry out effectively our authorized functions while ensuring that our activities that affect particularly US persons, and generally all persons, are carried out in a manner that protects the constitutional rights and privacy of such persons.

---

[189]E.O. 12333, Pt. 2.4, which states:

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

Chapter 7

ORGANIZATIONAL AFFILIATIONS AND CONTRACTING FOR GOODS AND SERVICES

Section I

Introduction

7-1. GENERAL.

a. Many DoD intelligence activities - like those of every foreign intelligence service - are clandestine in nature. Involved DoD intelligence personnel cannot travel, live, or perform their duties openly as DoD intelligence employees. Even in countries where United States intelligence works closely with cooperative foreign intelligence services, DoD intelligence personnel are often required by their hosts to conceal their United States intelligence status.

b. Accordingly, many professional intelligence personnel and organizations serving abroad, and even some serving in the United States, assume a "cover." Their employment by an intelligence organization is disguised and, to persons other than their families and co-workers, they are held out as employees of another government agency or of a commercial enterprise.[190]

7-2. COVER ARRANGEMENTS ARE ESSENTIAL.

a. The cover arrangements of intelligence organizations are essential to the performance of their foreign intelligence and counterintelligence missions. By definition, however, cover necessitates an element of deception which must be practiced within the United States as well as within foreign countries. This creates a risk of conflict with various regulatory statutes and other legal requirements.[191] In recognition of this risk, DoD 5240.1-R contains a number of controls which impact on cover arrangements and which attempt to ensure compliance with applicable laws and to minimize governmental intrusion on individual privacy.

b. Procedures 10 and 11, the subject of this chapter, are examples of those controls. In these areas where government finds it necessary to hide its presence, there also exists a potential for a chilling effect on open expression and debate. Governmental use of clandestine affiliation with its citizens must be con-

---

[190]See Report to the President by the Commission on CIA Activities Within the United States (1975) (hereinafter called Commission on CIA Report), at 215.

[191]Commission on CIA Report at 217.

strained to those circumstances where there exists a compelling state interest which justifies this predictable deterrent to First Amendment rights.[192] In the business of DoD intelligence (i.e., foreign intelligence collection, counterintelligence, counter-terrorism, operations security, etc.), this compelling interest derives from the fundamental precept that unless the Government protects its capacity to function and preserve the security of the nation, society could become so disordered that all rights and liberties would be endangered.

c. Individual freedoms and privacy are fundamental in our society. Constitutional government must be maintained. An effective and efficient intelligence system is necessary; and to be effective, many of its activities must be conducted in secrecy.[193]

d. Undisclosed participation by DoD intelligence components in organizations and contracting for goods and services without disclosure of the interest of DoD intelligence are classic activities of both the successful spy apparatus, and the Orwellian world of manipulated minds. It is no wonder that the constraints imposed by our intelligence oversight system in these areas reach an epoch in detail. But, despite their complexity, these constraints do not deter legitimate collection, nor impede necessary covert activity - they simply ask for a clear statement of the compelling reason for surreptitious conduct, and provide a reasonable means for control of the conduct to minimize the potential chilling effect on personal freedom.

---

[192]U.S. Const. amend. I.

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

[193]Commission on CIA Report at 5.

Section II

Procedure 10 - Undisclosed Participation in Organizations

7-3. SCOPE OF PROCEDURE 10.

a. Procedure 10 applies to the undisclosed participation of DoD intelligence personnel, as part of their official duties, in organizations in two broad categories:

(1) Any organization located within the United States.

(2) Any organization outside the United States which constitutes a "US person."[194]

b. Procedure 10 does not apply to an individual's involvement in an organization which is for solely personal purposes.[195] Participation in an organization may be primarily for personal purposes, but if even a small part of that involvement entails some action on behalf of the intelligence community, then the limitations and restrictions contained in Procedure 10 apply.[196]

7-4. REVIEW OF US PERSON ORGANIZATIONS.

a. Undisclosed participation on behalf of an intelligence component in any organization in the United States is subject to the provisions of Procedure 10, regardless of whether the organization constitutes a US person. Outside the United States only that participation in an organization which constitutes a US person is covered.

(1) This does not mean that DoD intelligence components have wholesale license to penetrate all non-US organizations outside the United States. It only means that Procedure 10 does not regulate such activity - mission objectives and operational constraints are always present. A bona fide mission must exist which dictates the participation of an DoD intelligence component in an organization, undisclosed, or otherwise. Absent that mission, such participation is not a valid use of intelligence resources.

---

[194]DoD 5240.1-R, Procedure 10, § A.

[195]DoD 5240.1-R, Procedure 10, § A.

[196]DoD 5240.1-R, Procedure 10, § B.6, states: "Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit." (Emphasis in the original.) It is not intended that the participation in organizations by intelligence personnel be regulated unless there is intelligence component sponsorship in that participation - even though the intelligence component may acquire some incidental benefit as a result of membership.

(2) Nevertheless, where the mission exists, enthusiasm need not be dampened, and undisclosed participation in non-US person organizations outside the United States, which appears appropriate to the mission, is not subject to Procedure 10.

b. A US person organization is --

(1) An unincorporated association substantially composed of US citizens or permanent resident aliens; or

(2) A corporation incorporated in the US, unless it is directed and controlled by a foreign government or governments.[197]

c. A corporation, a branch, an office, or a corporate subsidiary outside the United States, even if owned (wholly or partially) by a corporation incorporated in the US, is NOT a US person organization. Any organization that is located outside the United States may be presumed to NOT be a US person, unless specific information to the contrary is known to the DoD intelligence component.[198]

d. These distinctions are sometimes subtle, but they may be very important when conducting DoD intelligence activities outside the United States. For example, it is not unusual to see familiar US names in foreign countries. Even though there may exist some connection between that familiar name and a US person organization, it is not necessarily correct to presume that the entity using that name is a US person. Indeed, in almost all cases, the presumption would be incorrect. The use of a familiar US name abroad generally results from a licensing agreement with a foreign firm or the establishment of a legal entity under the laws of the country in which used. Rarely does that presence in a business mode constitute the existence of a US person organization. Consequently, it may be presumed that any organization outside the United States is not a US person unless specific information to the contrary is obtained.[199]

7-5. WHAT IS AN ORGANIZATION? For the purposes of Procedure 10, an organization can be virtually any group which has some sort of formal structure. Examples include the following:

a. Corporations and other commercial organizations;

b. Academic institutions;

---

[197]DoD 5240.1-R, Appendix A. ¶ 25.

[198]DoD 5240.1-R, Appendix A. ¶ 25.

[199]DoD 5240.1-R, Appendix A. ¶ 25.

c. Clubs;

d. Professional Societies;

e. Associations; and

f. Any other group whose existence is formalized in some manner, or otherwise functions on a continuing basis.[200]

7-6. WHAT CONSTITUTES PARTICIPATION?

a. Not all undisclosed participation in organizations comes under the purview of Procedure 10. First, as mentioned earlier, participation that is solely personal is not covered. Second, participation must be on behalf of an agency within the intelligence community to be covered.[201]

b. For the purposes of Procedure 10, participation includes any actions undertaken within the structure or framework of the organization. Service 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, are examples of activities which constitute participation.[202]

c. Participation is on behalf of an agency within the intelligence community, for Procedure 10 purposes, only when the participant is tasked or requested to take some action within an organization for the benefit of the requesting agency.[203] Thus, where it is necessary to conceal information about a person's intelligence affiliation solely because of reasons of operational cover, the provisions of Procedure 10 would not apply. If, on the other hand, the employee joins the organization in order to enhance cover, then Procedure 10 would apply. For example, case officer Brodrick is assigned to a remote location in the United States where she must establish cover as a businesswoman. Brodrick joins

---

[200]DoD 5240.1-R, Procedure 10, § B.2.

[201]DoD 5240.1-R, Procedure 10, § A.

[202]DoD 5240.1-R, Procedure 10, § B.4.

[203]DoD 5240.1-R, Procedure 10, § B.5. Actions undertaken for the benefit of an intelligence agency include collecting information, identifying potential sources of information, spotting contacts, or establishing and maintaining cover. If a cooperating source furnishes information to an intelligence component or one of its employees who is a participant in an organization with the cooperating source, this action is merely gratuitous unless the employee has been given prior direction or tasking by the intelligence component to collect such information.

a local business association. Her reason for joining is for personal purposes to learn more about commercial and fiscal matters, and all her expenses are paid out of her own pocket. Even though this membership will, as a by-product, support Brodrick's cover, unless actions are taken for the benefit of her intelligence agency in conjunction with that membership, the provisions of Procedure 10 do not apply. If, however, Brodrick joined the local association to enhance and maintain her cover, then such action has been undertaken on behalf of her agency and Procedure 10 applies.

d. In another example, suppose Brodrick's husband, who is an alfalfa broker, joins an international association of alfalfa merchants which has numerous members from foreign countries. Brodrick sees this as an excellent opportunity to spot and assess future sources. As a result, she is tasked by her commander to provide names of target country members of the association, which she secures during the association's social engagements while in company of her spouse. Brodrick's participation in the alfalfa association's activities, in this example, comes under the purview of Procedure 10.

e. It is important to note that there is a clear distinction between participation on behalf of an agency, and acting as a cooperating source to an agency.[204] While the former (participation on behalf of an agency) is constrained by Procedure 10, the latter (acting as a cooperating source) is not. Brodrick's spouse may furnish information about target country members of the alfalfa association to Brodrick, provided there has been no request for that information, either to Brodrick or her husband.[205] Neither Procedure 10, nor any other provision of DoD 5240.1-R, is intended to restrict the legitimate cooperation of persons with US intelligence activities. Any information of potential value to the United States may be received from cooperating sources by DoD intelligence components. In instances where this information is not within the jurisdiction of the DoD, then the information may be passed to an appropriate agency, and not retained in DoD intelligence files.[206] This principle applies to family members, to members of organiza-

---

[204]See DoD 5240.1-R, Procedure 2, § B.2.

[205]See DoD 5240.1-R, Procedure 10, § B.5. The threshold test for participation "on behalf" of an agency is slight. A person need merely be "tasked or requested to take action." DoD 5240.1-R, Procedure 10, is silent regarding notions of implied requests. It seems appropriate to apply a test of reasonableness to such notions. Accordingly, in the example in the text, if there is a course of conduct involving the spouses of intelligence operatives which shows an implied obligation to join organizations and pass information to the operative spouse, then it is arguable that such participation would be on behalf of the intelligence component. In such cases, it would be wise to secure the requisite approval for such "undisclosed" participation to assure that conduct does not run afoul of the spirit and intent of E.O. 12333 or DoD 5240.1-R.

[206]See DoD 5240.1-R, Procedure 3, § C and Procedure 4, § B.

tions, associations, etc., and even to walk-in sources at DoD intelligence offices.

7-7. ACTIONS OUTSIDE THE FORMAL STRUCTURE.

a. Finally, actions taken outside the organizational framework, such as attendance at meetings or social gatherings which involve organization members, but are not functions or activities of the organization itself, do not constitute participation.[207] So, if Brodrick does not otherwise join at the request of an intelligence agency and she confines her involvement with the alfalfa association to non-sponsored meetings, then her activities are not constrained by Procedure 10. If, however, any of the meetings involve business of the association, even though she is not a member, such as business luncheon meetings, or social affairs sponsored by the association, then her activity is governed by Procedure 10.

b. The key to identifying participation as being solely for personal purposes is whether it has been undertaken at the initiative and expense of the person involved, and for that person's benefit. If all three of these conditions apply, then participation is solely for personal purposes.

7-8. SUMMARY.

a. Participation in organizations is permitted by DoD intelligence personnel on behalf of any entity in the intelligence community only if the participant's affiliation with DoD intelligence is disclosed, or unless the undisclosed participation is approved as discussed in table 7-1.

b. Disclosure of the intelligence affiliation must 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. Disclosure on a membership application is sufficient to meet this requirement, and the disclosure may be made by the individual's organization, or by some other component in the intelligence community that is otherwise authorized to take such action on behalf of the cognizant DoD intelligence component.[208]

c. Disclosure, of course, is not required where the undisclosed participation has been approved as outlined in Procedure 10 and table 7-1.

---

[207]DoD 5240.1-R, Procedure 10, § B.4.

[208]DoD 5240.1-R, Procedure 10, § D.1.

Table 7-1
Undisclosed participation in organizations, DoD 5240.1-R, Procedure 10

GENERAL RULE: Participation by DoD intelligence personnel in organizations without disclosure of the participant's affiliation with a DoD intelligence component is permitted only within certain limitations and only after approval of a properly designated approval authority. 1/

LIMITATIONS	
1. Lawful purpose	Must be essential to achieving a lawful foreign intelligence or counterintelligence purpose of the DoD intelligence component's assigned mission
2. Within the United States	1. Not permitted to collect foreign intelligence about US persons 2. Not permitted to assess US persons as potential sources 2/
3. Duration of participation	No longer than 12 months 3/
4. Influencing activities of the organization or its members	Not permitted unless approved in advance by the DUSD(P) with concurrence of the DoD General Counsel 4/
APPROVAL AUTHORITIES	SCOPE OF APPROVAL AUTHORITY
DoD Intelligence Components	1. Participation in meetings open to the public 2. Participation where other known to the organization to be US government personnel participate 3. Participation in professional or educational groups for personal enhancement or improvement 4. Participation in seminars and meetings where disclosure of affiliation is not required
Senior DoD Intelligence Officials, or their single designees 5/	All other purposes within the mission of the collecting DoD intelligence component 6/

Table 7-1
Undisclosed participation in organizations, DoD 5240.1-R, Procedure 10

NOTES:

1/ Procedure 10 is limited in scope to participation by DoD intelligence personnel in any organization within the United States, or to any organization outside the United States that constitutes a United States person, and further limited in application to circumstances in which the participation is on behalf of an agency in the intelligence community. Participation which is solely for personal purposes (i.e., undertaken at the initiative and expense of the person involved for that person's benefit) is not covered by DoD 5240.1-R, Procedure 10.

2/ This does not preclude the collection of information about such United States persons, volunteered by cooperating sources participating in organizations to which such persons belong, provided such collection is otherwise authorized under DoD 5240.1-R, Procedure 2.

3/ Participation which lasts longer than 12 months must be re-approved by the appropriate approving official on an annual basis.

4/ DoD intelligence component personnel may not be authorized to participate in organizations for the purpose of influencing their activities or the activities of their 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 US persons and it is reasonably believed to be acting on behalf of a foreign power. Requests for participation in these circumstances must be forwarded to the Deputy Under Secretary of Defense (Policy) (DUSD (P)), setting forth the relevant facts justifying such participation and explaining the nature of the contemplated activity.

5/ For the purposes of DoD 5240.1-R, Procedure 10, these officials are the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Assistant Chief of Staff for Intelligence, Department of the Army; the Commanding General, US Army Intelligence and Security Command; the Director of Naval Intelligence; the Director of Intelligence, US Marine Corps; the Assistant Chief of Staff, Intelligence, US Air Force; the Director, Naval Investigative Service; and the Commanding Officer, Air Force Office of Special

Table 7-1
Undisclosed participation in organizations, DoD 5240.1-R, Procedure 10

Investigations. These officials may designate a single designee to also exercise this approval.

6/ For the purposes of DoD 5240.1-R, Procedure 10, these include the following:

a. Collection of significant foreign intelligence outside the United States, or from or about other than US persons within the US, provided no information involving domestic activities of the organization or its members may be collected.

b. Counterintelligence purposes at the written request of the Federal Bureau of Investigation (FBI).

c. Collection of significant counterintelligence about other than US persons, or about US persons who are within the investigative jurisdiction of the Department of Defense, provided any such participation that occurs within the US must be coordinated with the FBI.

d. Collection of information necessary to identify and assess other than US persons as potential sources of assistance for foreign intelligence and counterintelligence activities.

e. Collection of information necessary to identify US persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

f. Activities required to develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities.

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

Section III

Procedure 11 - Contracting for Goods and Services

7-9. SCOPE OF PROCEDURE 11.

a. DoD 5240.1-R, Procedure 11, applies to contracting or other arrangements with United States Persons for the procurement of goods and services by or for DoD intelligence components within the United States. It does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. Contracts for enrollment of students in academic institutions, wherein non-disclosure of intelligence component sponsorship is necessary, are covered by Procedure 10.[209]

b. In addition, Procedure 11 does affect government contracting methodology. In almost all cases, when an intelligence component contracts for goods and services it must follow the provisions of the Federal Acquisition Regulation (FAR), and the Department of Defense supplement to the FAR. Limited exceptions are permitted to this general rule in certain acquisitions. Consult your supporting judge advocate or legal advisor for assistance with specific questions.

7-10. AN AFFIRMATIVE DISCLOSURE RESPONSIBILITY.

a. At first blush, Procedure 11 also seems to have an enormous reach and its implications suggest an affirmative responsibility to disclose DoD intelligence sponsorship in virtually all procurement areas. While such an affirmative responsibility does, in fact, exist with respect to contracting with academic institutions,[210] there are a number of expressed and implied exceptions to disclosure in other contracts.

b. First of all, disclosure is not required when a contract is for published material available to the general public, or for routine goods or services necessary for the support of approved activities. Examples expressed in the text of Procedure 11 include credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities. Implied exceptions would be any reasonable acquisition incident to approved activities. For example, where there exists an approved operational plan, contracting for matters incident to

---

[209]DoD 5240.1-R, Procedure 11, § A.

[210]See DoD 5240.1-R, Procedure 11, § B.1., which implements that portion of E.O. 12333, Pt. 2.7, which states that "(c)ontracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution."

the support of that plan may be done without revealing the sponsorship of the DoD intelligence component.[211]

7-11. CONTRACTING WITH OTHER GOVERNMENT AGENCIES.

a. As mentioned earlier, Procedure 11 does not apply to contracting with government entities. This most frequently occurs at the Federal agency level. The Economy Act of 1932, as amended,[212] permits US government departments to place orders with one another "for materials, supplies, equipment, work, or services, of any kind that such requisitioned Federal agency may be in a position to supply or equipped to render..." A 1982 amendment to the Act requires that both the ordering agency (i.e., the one placing the order) and the contracting agency (i.e., the one with the contract with the commercial entity) must be authorized to procure the item or service in question, and the Act cannot be used to circumvent the conditions and limitations on funds applicable to either the ordering or requisitioned agency.[213]

b. So long as these Economy Act transactions are for published materials available to the general public, or for routine goods or services necessary to the support of approved activities, they may be conducted without revealing the sponsorship of the intelligence component.[214] If, on the other hand, the contract involves other matters, the sponsorship must be disclosed, or approval must be secured to conceal that sponsorship. This is because the coverage of Procedure 11 includes contracting "by or for" a DoD intelligence component. In the case of an Economy Act transaction, the use of another government agency constitutes contracting "for" an intelligence component.[215]

c. Contracting "with government entities" is not covered by Procedure 11.[216] In those cases, it is unnecessary to disclose sponsorship to the government entity with which the intelligence component is contracting. The most prevalent example of contracting with another government entity is found in industrial

---

[211]DoD 5240.1-R, Procedure 11, § B.2.a.

[212]31 U.S.C. § 1535.

[213]31 U.S.C. § 1535.

[214]DoD 5240.1-R, Procedure 11, § B.2.a.

[215]DoD 5240.1-R, Procedure 11, § B.2.a.

[216]DoD 5240.1-R, Procedure 11, § A.

funded activities. These include, for example, the laboratory and depot repair services of the Army Materiel Command.[217]

d. Although contracting with government entities will most frequently occur at the Federal level, there are, of course, other instances in which contracting is done with other governments - other nations - and even with state governments in the United States. Procedure 11 does not apply to those contracting arrangements; however, other restrictions or provisions of DoD 5240.1-R may have applications. For example, Procedure 10 (Undisclosed Participation in Organizations) could apply in the event that the contract involved "participation" within the meaning of that procedure, and provided the entity involved constituted a US person.[218]

7-12. APPROVAL AUTHORITIES.

a. Other than these expressed and implied exceptions, when contracting for goods or services by or for a DoD intelligence component, with US persons within the United States, or with contractors abroad who are US persons, sponsorship must be revealed, unless there is a written determination that such sponsorship must be concealed to protect the activities of the DoD intelligence component involved. The authority to make this determination is limited to 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).

---

[217]There are three types of contracts associated with dealing with industrial funded activities. Two are internal to the government (project orders and service orders) and are treated as contracts not subject to the FAR. The third, standard commercial contracts, is subject to the FAR. Procedure 11 is not clear with respect to disclosure of sponsorship in the third type contract. It is probable that if the requiring intelligence component is knowledgeable in advance that the industrial funded activity will use a commercial contract, disclosure is required. On the other hand, where the commercial contracting decision and choice is solely within the discretion of the industrial funded facility, it seems reasonable to conclude that a forced disclosure would be too strict an interpretation of Procedure 11. Cf. E.O. 12333, Pt. 2.7, which expressly authorizes intelligence agencies to enter into contracts or arrangements without revealing their sponsorships.

[218]See DoD 5240.1-R, Procedure 11, § A. The precise wording of § A, inter alia, is "(t)his procedure does not apply to contracting with government entities." There is nothing in E.O. 12333 or DoD 5240.1-R to suggest that there is any intent to restrict contracting with non-federal government entities. Indeed, because the underlying principles for regulating intelligence activities concern the protection of constitutional and privacy rights of persons, and because government entities are not persons in the eyes of the law, it seems reasonable to conclude that restrictions on undisclosed sponsorship do not extend to contracts DoD intelligence components have with such non-federal government entities.

b. The form of such a written determination need not be a specific request generated under DoD 5240.1-R, Procedure 11. Indeed, in most cases, such a determination will have been made in some other fashion, such as in the promulgation of a regulation or directive. In addition, where activities are carried out pursuant to an operations plan which has been approved by one of those officials, and that operations plan includes provisions covering concealed sponsorship of contracting or acquisition, then the operations plan will satisfy this requirement.

d. It is important to seek legal advice when contracting may involve, or may require, concealment - or even lack of disclosure - of DoD intelligence sponsorship of a particular contracting activity. The advice of a supporting judge advocate or legal advisor may be necessary to assure compliance with Procedure 11, and/or adequate protection of sensitive relationships in the contracting process. Government contracting is a complex and sometimes frustrating business. In the intelligence and counterintelligence arena it is even more complicated by myriad extraordinary procedural and funding implications. Legal advice often will be vital to assure mission accomplishment.

e. See table 7-2 for a display of the limitations and approval requirements for contracting for goods and services without revealing sponsorship by an DoD intelligence component.

Table 7-2
Contracting for goods and services, DoD 5240.1-R, Procedure 11

GENERAL RULE: Contracting for goods and services with US persons by DoD intelligence components, without revealing the sponsorship of that component, is permitted only in certain circumstances, unless a determination has been made in writing by a designated official that such sponsorship must be concealed to protect the activities of the DoD intelligence component concerned. 1/

GENERAL LIMITATIONS	
1. Contracts with academic institutions 2/	Disclosure of the fact of sponsorship by DoD intelligence component is required to appropriate institution officials prior to the making of a contract.
2. Contracts with commercial organizations, private institutions and private individuals 3/	May be done without revealing the sponsorship of the intelligence component if the contract is for -- a. Published material available to general public. b. Routine goods or services necessary to support of approved operations or activities. c. Other items incident to approved operations or activities.
OTHER CIRCUMSTANCES	
3. Written determination by a. Secretary or Under Secretary of a Military Department b. Director, National Security Agency c. Director, Defense Intelligence Agency or d. Deputy Under Secretary of Defense (Policy) 4/	That the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned.

Table 7-2
Contracting for goods and services, DoD 5240.1-R, Procedure 11

NOTES:

1/ Procedure 11 applies to contracting with US persons within the United States, and contracting abroad with contractors who are US persons. It does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. (Procedure 10 applies to enrollment of students in academic institutions.)

2/ Both private and public academic institutions are covered. Contracts with individuals who may be affiliated with academic institutions, and contracts with research elements which are affiliated with academic institutions but which are separate legal entities, are considered contracts with commercial organizations, private institutions and private individuals. Prior disclosure to institutional officials is not required in these circumstances, and in similar circumstances where the academic institution is not a party to the contract.

3/ Procedure 11 does not apply to contracting arrangements made with other government entities.

4/ Written determination may be included in approved operations plans, regulations or directives. In some instances, such written determinations may also be found in approved Operations Security Plans or Security Classification Guides. The determination, however, must have been made by or in the name of one of the officials listed.

Section IV

Conclusion

7-13. CONSTITUTIONAL OBJECTIVES. Restrictions on intelligence components regarding concealing participation in organizations and sponsorship of contracting activities are essential elements in the preservation of Constitutional objectives enunciated in the Bill of Rights. In 1975, the Commission on CIA Activities Within the United States, chaired by Nelson A. Rockefeller, noted that the Supreme Court of the United States has outlined the following Constitutional doctrines in this regard:[219]

a. Any intrusive investigation of an American citizen by the government must have a sufficient basis to warrant the invasion caused by the particular investigative practices which are utilized;

b. Government monitoring of a citizen's political activities requires even greater justification;

c. The scope of any resulting intrusion on personal privacy must not exceed the degree reasonably believed necessary;

d. With certain exceptions, the scope of which are not sharply defined, these conditions must be met, at least for significant investigative intrusions, to the satisfaction of an uninvolved governmental body such as a court.

7-14. OVERSIGHT OF INTELLIGENCE ACTIVITIES. These concepts have, since 1975, become fundamental precepts in the oversight process for United States intelligence activities, along with the realization that individual liberties depend on maintaining public order at home and in protecting the country against infiltration from abroad and armed attack. Government has both the right and the obligation within Constitutional limits to use its available power to protect the people and their established form of government. A vital part of this protection is an effective intelligence service and counterintelligence program, directed toward accurate forecasting of our adversaries, and ascertaining the activities of their foreign intelligence services. Concealment of our intelligence involvement in certain activities is essential to that effectiveness.

---

[219]Commission on CIA Report at 3 & 4.