

~~FOR OFFICIAL USE ONLY~~

TRANSITION BOOK

**ASSISTANT TO THE SECRETARY OF DEFENSE
(INTELLIGENCE OVERSIGHT)**

DECEMBER 2000

~~FOR OFFICIAL USE ONLY~~



INTELLIGENCE
OVERSIGHT

ASSISTANT TO THE SECRETARY OF DEFENSE
4035 RINGGOLD ROAD, SUITE 210
FAIRFAX, VIRGINIA 22030

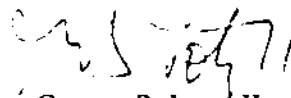
December 22, 2000

MEMORANDUM FOR EXECUTIVE SECRETARY, DEPARTMENT OF DEFENSE
ATTN: COLONEL MARIA L. CRIBBS

SUBJECT: Transition Books

In response to your memorandum dated December 14, 2000, same subject as above, I have attached three transition books for the preparation of DoD leadership in the next Administration.

The point of contact for the Intelligence Oversight transition books is Mr. Steven A. Cantrell, the Deputy ATSD(IC). He can be reached at (o) 703-275-6561 or (h) 703-912-1830. If unavailable, please contact me directly at (o) 703-275-6560 or (h) 703-281-0014.


George B. Loug II

Attachments



INTELLIGENCE
OVERSIGHT

ASSISTANT TO THE SECRETARY OF DEFENSE
4035 RIDGETOP ROAD, SUITE 210
FAIRFAX, VIRGINIA 22030

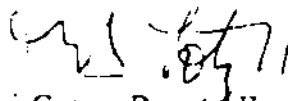
December 22, 2000

MEMORANDUM FOR EXECUTIVE SECRETARY, DEPARTMENT OF DEFENSE
ATTN: COLONEL MARIA I. CRIBBS

SUBJECT: Transition Books

In response to your memorandum dated December 14, 2000, same subject as above, I have attached three transition books for the preparation of DoD leadership in the next Administration.

The point of contact for the Intelligence Oversight transition books is Mr. Steven A. Cantrell, the Deputy ATSD(10). He can be reached at (o) 703-275-6561 or (h) 703-912-3830. If unavailable please contact me directly at (o) 703-275-6560 or (h) 703-281-0014.


George B. Jones II

Attachments
Book 3 of 3

Q

Q

Q

~~FOR OFFICIAL USE ONLY~~

ASSISTANT TO THE SECRETARY OF DEFENSE
(INTELLIGENCE OVERSIGHT)
TRANSITION BOOK

TABLE OF CONTENTS

	PAGE
I. (U) ORGANIZATION AND MANAGEMENT	1
A. (U) Organization	1
1. (U) Mission Statement	1
2. (U) Organization Structure	1
3. (U) Goals	2
4. (U) Functions	2
B. (U) Management	4
1. (U) Chain of Command	4
2. (U) Regulatory Authority	4
3. (U) Management Studies and Issues (none)	5
C. (U) External Process	5
1. (U) Executive – Key Interagency Relationships	5
2. (U) Congressional	5
a. (U) Key Reports (none)	5
b. (U) Critical Reports to Congress (none)	5
c. (U) Pending Legislative Issues (none)	5
II. (U) BUDGET	6
A. (U) Budget Review	6
B. (U) Budget Detail	6
1. (U) Personnel	6
2. (U) Office Equipment	6
3. (U) Travel	6
4. (U) Contractor Support	6
C. (U) Budget Trends	6
D. (U) Budget Issues	6

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

ASSISTANT TO THE SECRETARY OF DEFENSE
(INTELLIGENCE OVERSIGHT)
(ATSD(IO))

I. (U) ORGANIZATION AND MANAGEMENT

A. (U) Organization

1. (U) **Mission Statement:** The ATSD(IO) provides the Secretary of Defense with independent oversight of all DoD's intelligence, counterintelligence, and intelligence-related organizations, as well as all intelligence activities performed by non-intelligence units, to ensure their activities are conducted in compliance with federal law, executive orders, presidential directives, DoD directives, regulations, policies and standards of conduct. The ATSD(IO) provides a written report quarterly to the Secretary of Defense and, in turn, to the Intelligence Oversight Board of the President's Foreign Intelligence Oversight Board (expanded detail in section C.1). The ATSD(IO) also develops and implements intelligence Oversight policy in coordination with the DoD General Counsel.

2. (U) **Organizational Structure:** A component of the Office of the Secretary of Defense, the Office of the ATSD(IO) consists of eleven personnel (expanded detail in paragraph III. A.). The ATSD(IO) reports directly to the Secretary and Deputy Secretary of Defense. There are no subordinate organizations under the Office of the ATSD(IO); however, there is an aggressive partnership with the intelligence staffs and activities of the Joint Staff, Combatant Commands, Military Services, and Defense intelligence agencies (National Security Agency (NSA), Defense Intelligence Agency (DIA), National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA)) in the management and direction of the DoD Intelligence Oversight program. In addition, as warranted, the ATSD(IO) may request temporary assistance from these same organizations in the form of personnel, facilities, and other services.

(U) The Office of the ATSD(IO) is integrated within OSD, reporting directly to the Secretary of Defense, to reflect the importance the Secretary assigns to this function. This office was established by the Secretary of Defense in 1976 (in implementation of an Executive Order on U.S. Intelligence Activities) following the DoD's spying on civil rights and anti-Vietnam war demonstrators during the 60s and early 70s. What had begun as a legitimate force protection mission, evolved, through mission creep, into an abuse of the Constitutional rights of *U.S. persons* by Defense intelligence and counterintelligence personnel. Since 1976, the ATSD(IO) has been charged with preventing a recurrence of these types of transgressions.

(U) *The term U.S. person means more than just a U.S. citizen. It includes an alien known by the DoD intelligence component concerned to be a permanent resident alien, and a corporation incorporated in the U.S. An expanded legal definition is contained in Executive Order 12333 (TAB A, paragraph 3.4.i).*

~~FOR OFFICIAL USE ONLY~~

3. (U) Goals:

a. (U) To ensure Defense intelligence units and counterintelligence and non-intelligence units performing intelligence activities do not infringe on or violate the individual rights of U.S. persons guaranteed by the Constitution and the laws of the United States.

b. (U) To ensure those directing and conducting Defense intelligence activities are doing so within the guidelines established under Executive Order (EO) 12333, "United States Intelligence Activities" (TAB A), and DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons" (TAB B).

c. (U) To ensure, through an aggressive multi-media awareness, education, and training program, that those involved with intelligence activities are aware of the restrictions imposed by EO 12333 and DoD 5240.1-R; and more importantly, that Intelligence Oversight is, in fact, an enabler which maximizes the effectiveness of Defense intelligence assets.

d. (U) To ensure DoD senior leadership, particularly as it grapples with new domestic missions, e.g., Joint Task Force-Civil Support, remains cognizant of the legal restrictions against tasking intelligence assets inappropriately against U.S. persons.

e. (U) To ensure future leaders of emerging democracies understand the concepts, importance, and applicability of Intelligence Oversight. This is accomplished through a proactive education program in concert with the Marshall Center, the NATO School, and the new Western Hemisphere Institute for Security Cooperation (follow-on to the School of the Americas).

f. (U) To ensure evolving intelligence and/or related capabilities (e.g., use of the Internet and information operations) are developed with a thorough understanding of Intelligence Oversight.

4. (U) Functions: The ATSD(IO) is charged by the Secretary of Defense with ensuring DoD's intelligence assets do not, during the course of accomplishing their mission, violate the Constitutional rights of U.S. persons. In order to effectively perform this mission, the ATSD(IO) has, under DoD Directive 5148.11 (TAB C), independent oversight of all Defense intelligence and counterintelligence units and non-intelligence units performing intelligence activities. The Secretary of Defense has recognized and directed that the ATSD(IO) have complete and unimpeded access to all intelligence, counterintelligence or intelligence-related facilities, units, operations, activities, and files regardless of classification, compartmentation, or special access. It is under this rubric that the ATSD(IO) performs the following functions in the management and direction of the Defense Intelligence Oversight program:

a. (U) Develops Intelligence Oversight policy and, in coordination with the DoD General Counsel, issues guidance, including regulatory guidance implementing Intelligence Oversight aspects of E.O. 12333, which was issued in 1981. The DoD

regulation, DoD 5240.1-R, signed by both the Attorney General and Secretary of Defense and issued in 1982, does not specifically address many of today's issues. As a result, the ATSD(IO) in coordination with the DoD General Counsel, the Military Departments, Joint Staff and others as appropriate is issuing policy modules to clarify Intelligence Oversight concerns in such evolving areas as force protection, use of the Internet by intelligence professionals, and Information Operations (expanded detail in section IV. A.).

b. (U) Monitors and evaluates the effectiveness of the Intelligence Oversight orientation and training programs of the Joint Staff, Combatant Commands, Military Services, and Defense intelligence agencies. This includes operationally deployed U.S. units operating in multinational organizations such as NATO.

c. (U) Conducts rigorous and independent inspections of Defense intelligence activities worldwide, ranging from large staffed organizations such as the National Security Agency to deployed tactical intelligence activities such as those operating in the Balkans and Arabian Peninsula. These inspections are based on priorities derived from Presidential and Defense intelligence priorities, CINCPAC's priorities, current policy objectives, areas of high personnel turnover (e.g., Southwest Asia, Korea, and Bosnia), and areas of high potential risk (e.g., CONUS force protection, support to law enforcement agencies, and information operations).

~~(FOUO)~~ The Office of the ATSD(IO) conducted compliance inspections of 155 units in the U.S. and overseas in 21 countries as well as 99 staff visits. During visits to U.S. embassies, in addition to the inspection of Defense intelligence assets, the ATSD(IO) meets with the Ambassador and CIA Chief of Station to discuss the relationship and quality of support provided by the Defense intelligence assets.

d. (U) Provides the Secretary of Defense and senior leadership an independent assessment of the mission and management performance of Defense intelligence organization. This is accomplished through the ATSD(IO)'s comprehensive access to worldwide DoD intelligence activities, coupled with a Secretary of Defense-level perspective. This not only provides the Secretary of Defense with the current state of Defense Intelligence, it also provides the ATSD(IO) an avenue to provide inspection observations to the appropriate unit's parent agency for resolution, information, and/or commendation.

e. ~~(FOUO)~~ Reviews and monitors, under the purview of DoD Directive S-5210.36, sensitive DoD support to other DoD components and other Departments and Agencies of the U.S. Government.

f. (U) Conducts special inquiries into allegations of questionable or improper activities by Defense intelligence components (see ECEHLON Report, TAB D). As appropriate, the ATSD(IO) directs DoD components to investigate allegations of illegal or improper activities by intelligence elements.

g. (U) Reviews and analyzes reports of questionable activities received from DoD intelligence components, their general counsel, and the inspectors general of the Joint Staff, Combatant Commands, Military Services, and Defense intelligence agencies.

h. (U) Audits intelligence commercial activities (ICAs). Sections 431-437 of USC Title X, authorize DoD to conduct ICAs and require an annual audit of all DoD ICAs. DoDD 5240.12, "Department of Defense Intelligence Commercial Activities," (2 Dec 92) tasks the ATSD(IO), as a disinterested office, to conduct these audits. It further requires that the ATSD(IO) audit report be furnished to ASD(C3I) for Congressional reporting purposes.

i. (U) Reports quarterly in writing and in close coordination with the DoD General Counsel, to the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board (TAB E) (see section C.1. below for additional detail).

j. (U) Coordinates, as appropriate, with the DoD Inspector General on matters relating to the Inspector General's areas of responsibility in accordance with DoD Directive 5106.1. The ATSD(IO) is responsible to the Executive Branch while the statutory DoD Inspector General is responsible to Congress. The ATSD(IO) has oversight of the intelligence related activities of the DoD Inspector General.

k. (U) Performs independent studies for the Secretary of Defense as directed (see Mitre Report in section IV.B.1).

l. (U) Conducts an aggressive Intelligence Oversight outreach program to educate senior DoD leadership on responsibilities associated with the use of intelligence assets.

m. (U) Provides Intelligence Oversight instruction to the Marshall Center, the NATO School and the new Western Hemisphere Institute for Security Cooperation, for the education of military and civilian leaders of emerging democracies (see TAB F).

B. (U) Management

1. (U) **Chain of Command:** The ATSD(IO) reports directly to the Secretary and Deputy Secretary of Defense in the accomplishment of his independent oversight mission. In consultation with the General Counsel, the ATSD(IO) is required to report at least quarterly to the Secretary of Defense and to the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board (TAB E).

2. (U) **Regulatory Authority:** The basic authority document for the ATSD(IO) is DoD Directive 5148.11 (TAB C). This charter affords excellent operational flexibility and unhindered access to intelligence functions, intelligence-related information, and intelligence personnel, regardless of classification or compartmentation. It authorizes the ATSD(IO) to communicate directly with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, and the Directors of Defense intelligence agencies and their respective inspectors general. In addition, the ATSD(IO)

coordinates with the DoD Inspector General on matters relating to his area of responsibility in accordance with Public Law 95 452.

3. (U) Management Studies and Issues: None

C. (U) External Process

1. (U) Executive--Key Interagency Relationships: The ATSD(IO) is the designated DoD point of contact with the Intelligence Oversight Board (IOB) of the President's Foreign Intelligence Advisory Board (TAB E). As such, the ATSD(IO) is responsible for the DoD's Quarterly Intelligence Oversight Report submitted to the IOB, after approval by the Secretary of Defense. This report is prepared in coordination with the DoD General Counsel and describes significant DoD Intelligence Oversight responsibilities. In addition, it includes the Intelligence Oversight submissions of the Joint Staff, the Military Services, and Defense intelligence agencies.

(U) DoD's keystone document of Intelligence Oversight is DoD regulation 5240.1-R. (TAB B), which provides the foundation for Intelligence Oversight guidance issued to all Defense components. The Secretary of Defense issued the document after it was approved by the Attorney General as stipulated by E.O. 12333. This approval process reflects the unique working relationship the Secretary of Defense and Attorney General share in the Intelligence Oversight arena.

(U) Since 1976, this office has provided a continuous and distinct reporting channel for the Secretary of Defense within the Executive Branch. Unlike the statutory DoD Inspector General, who is required by law to report to Congress, the ATSD(IO) reports only through the Secretary of Defense to the IOB.

(U) The ATSD(IO) is an active participant with the Inspectors General of the Defense intelligence organizations and CIA in an international forum (U.S., U.K., Canada, Australia, New Zealand, Belgium, and South Africa) of intelligence review agencies. The next meeting will be held in Washington D.C. in October 2001.

2. (U) Congressional: Questionable activities of a serious nature reported to the ATSD(IO) through Intelligence Oversight channels or determined during inspections and/or investigations are immediately reported to the Secretary of Defense, to the IOB and, as appropriate, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) for reporting as necessary to the Congress or its pertinent committees, and/or the DoD IG. In addition, the ATSD(IO) provides ICA audit results to ASD(C3I) for Congressional reporting.

a. Key Committees: None

b. Critical Reports to Congress: None

c. Pending Legislative Issues: None

II. (U) BUDGET

A. (U) Budget Overview: The ATSD(IO) has no external budget program responsibilities.

B. (U) Budget Detail:

1. **(U) Personnel:** The personnel budget for the ATSD(IO), which is administered by the Budget and Finance Office, Washington Headquarters Services (WHS), is \$847,993.

2. **(U) Office Equipment:** The ATSD(IO) budget for FY 2001 is \$76,600. Funding for the maintenance of copiers, facsimile machines and associated office equipment is provided through the Budget and Finance Office, WHS.

3. **(U) Travel:** The ATSD(IO) has been allocated a travel target of \$125,000 for FY 2001. Travel funds are used to support both inspections and investigations.

4. **(U) Contractor Support:** The ATSD(IO) maintains a contract with ACS Inc., \$238,000 for FY 2001, to support its mission. The contract provides assistance in developing policy, planning and execution support to the inspection process.

C. (U) Budget Trends: The ATSD(IO) budget has remained relatively constant with the exception of increased travel and contract support. Contract support should remain relatively constant. As the Military Services downsize and cut personnel, we find that individuals responsible for Intelligence Oversight are being cut as well. As a result, the ATSD(IO)'s active inspection and investigations program continues to compensate for these drawdowns.

D. (U) Budget Issues: None.

III. (U) PERSONNEL

A. (U) Summary Statistics: The Office of the ATSD(IO) is staffed with eleven full-time employees and two part-time consultants as follows: ATSD(IO) (ES-6), Deputy ATSD(IO) (ES-02), five Assistants for Inspections (4 GS-15s and 1 GS-12), Counsel (GS-15), one Administrative Officer (GS-12), one Secretary (GS-8), one contract employee, and two part-time consultants who bring unique expertise to current issues. The ATSD(IO) is authorized to obtain assistance from DoD components for the conduct of audits, inspections, and/or investigations.

B. (U) Personnel Management Issues: Historically, the Office of the ATSD(IO) has had a full-time NSA and CIA office assigned (these are two-year rotational positions). The experience and insights these individuals bring to the ATSD(IO)'s mission, particularly as it relates to their agencies, is invaluable. Since October 1999, the DIA position has gone unfilled. The ATSD(IO) is working with the Director of DIA to fill this critical position.

IV. (U) POLICY ISSUES:

A. (U) Overview of the Policy Development Process: The ATSD(IO) develops Intelligence Oversight policy and, in coordination with the DoD General Counsel, issues guidance, including regulatory guidance implementing Intelligence Oversight aspects of E.O. 12333 and DoD Regulation 5240.1-R. To address rapidly evolving Intelligence Oversight issues, the ATSD(IO) uses policy modules, which are developed in coordination with the DoD General Counsel, the Military Departments, Joint Staff and others as appropriate.

1. (U) Force Protection: The ATSD(IO) issued policy guidance (TAB G) in December 1998, to the DoD on intelligence collection, reporting, analysis, and dissemination of U.S. person-related material which impacts upon force protection. This policy guidance was necessary following the Khobar Towers and Oklahoma City bombings where some military commanders, trained to rely on their intelligence staffs for threat information, began to inappropriately task the intelligence community for information they needed to protect their people and resources. Frequently this meant that Defense counterintelligence assets were directed to collect information on local criminal and dissident groups in the CONUS. Since E.O. 12333 and DoD Regulation 5240.1-R prohibit the collection of domestic threat information unless a foreign connection exists, such direction and any response are illegal. In lieu of a foreign connection, such threatening activity is criminal, not international terrorist, activity. Commanders must obtain information on criminal threat from military or civilian criminal investigative organizations (e.g., OSI, NCIS, FBI, and local law enforcement). However, if Defense intelligence or counterintelligence assets become aware of any information concerning threats, they are enjoined to pass that information immediately to the concerned commander and security forces. To alleviate any confusion regarding support to a commander's force protection mission, the ATSD(IO) published specific guidance detailing the support a commander could expect from the intelligence community and describing the permissible support Defense intelligence could provide.

2. (U) Defense Intelligence Support to Civil Authorities: Homeland defense is a broad concept that has large civil as well as military components. The Unified Command Plan (1999) established Joint Task Force Civil Support (JTF-CS), under Joint Forces Command, in order to increase DoD's readiness to respond in the event of a weapons of mass destruction incident within the U.S., its territories, or possessions. In preparing for this critical mission, the ATSD(IO) has been working closely with the ATSD (Civil Support)'s staff and the Joint Staff to ensure those involved in the process understand where and when the Defense Intelligence Community may provide support. This issue was highlighted during a recent Congressionally directed exercise, TOP OFF, when the JTF-CS commander attempted to obtain domestic operational and threat data from the Defense Intelligence Community as opposed to the law enforcement community. The Defense Intelligence Community is restricted from collecting information on domestic activities that have no foreign connection. This restriction which is reflected in E.O. 12333 and DoD Regulation 5240.1-R evolved from a very similar situation in the 60s and 70s.

(U) Beginning in the 60s U.S. Army commanders were given the mission under the Garden Plot Operations Order, to prepare for civil unrest in the U.S. The DoD asked the FBI for information on the local threat in the 40 largest U.S. cities, but the FBI declined to provide it. The Army then set about using its intelligence and counterintelligence units and personnel to collect all manner of domestic information to include the names and addresses of mayors, influential citizens, church leaders, as well as local civil rights protestors and anti-war activists. It was the collection and maintenance of this data (and abuses committed by the CIA) that led to Congressional hearings and focused the nation's attention on the illegal domestic activities of the Intelligence Community. To prevent a recurrence of this type of activity, E.O.s have been issued (the latest is E.O. 11333) and the Secretary of Defense issued, after approval of the Attorney General, DoD 240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons."

(U) The ATSD(IO) is working closely with the ATSD(CS) and the Joint Staff to publish authoritative guidance (the TOP OFFICIAL After Action Report, a CJCS Instruction, and a JCS CONPLAN) describing the methodology by which a commander can obtain information needed for military operations, support to civil authorities, and force protection in CONUS. The guidance will reinforce the role of local government, National Guard, and military and civilian criminal investigative organizations in the provision of information on entities without a demonstrable foreign connection.

3. (U) **Use of the Internet:** The ATSD(IO) is, with assistance from the DoD General Counsel, developing Intelligence Oversight guidance for intelligence and counterintelligence use of the Internet. In addition to general principles, the policy guidance will include specific provisions for intelligence and counterintelligence personnel to analyze and characterize e-mail addresses, web sites, i.e., Uniform Resource Locators (URLs), and Internet Protocol (IP) addresses.

4. (U) **Counternarcotics:** In early 2000, the ATSD(IO) began a review of the adequacy of available guidance to the Defense Intelligence Community components supporting drug law enforcement agencies (DLEAs). Staff members visited Joint Interagency Task Forces East and West, Joint Task Force 6, the Defense Intelligence Agency, and the Office of the Deputy Assistant Secretary of Defense (Drug Enforcement Policy and Support). Interviews were conducted with personnel involved in providing intelligence support to, as well as with DLEA individuals. The focus of this effort, conducted at both policy and working levels, was to assess their understanding of and compliance with Intelligence Oversight guidance. During this process, several violations were discovered which were quickly corrected. It was determined that these violations were the result of improper interpretation of Intelligence Oversight guidance, not due to a lack of guidance. The Office of the ATSD(IO) will continue to monitor and work with intelligence units in the field to ensure continued understanding and compliance with Intelligence Oversight regulations.

B. (U) Major Policy Issues requiring attention in the next few months:

1. ~~(FOUO)~~ MITRE Report on "Iraqi Chemical Warfare: Analysis of Information Available to DoD (U)":

- ~~(FOUO)~~ Completion of MITRE Report: study directed by former Deputy Secretary of Defense
- ~~(FOUO)~~ Task was to determine US knowledge of Iraqi chemical warfare capability and what DoD did with the information.
- ~~(FOUO)~~ Results were provided to Secretary and Deputy Secretary of Defense
- ~~(FOUO)~~ Follow-up action required: one of the ATSD(IO)'s recommendations to SECD EF (along with the basic MITRE Report as well as in a GC coordinated declassification plan) was to approve ATSD(IO)-directed/ conducted declassification action on first five sections of the MITRE Report. Declassification would
- ~~(FOUO)~~ Assure our Gulf War veterans of the integrity of the study effort and that DoD had made public all pertinent information;
- ~~(FOUO)~~ Satisfy Freedom of Information Act (FOIA) requests for release of the MITRE Report. Specifically, Mr. Patrick Eddington, former CIA analyst, filed a FOIA request for the draft MITRE report. Working with the DoD General Counsel and the Department of Justice, the ATSD(IO) withheld release of the draft report, asserting rights under the classified document FOIA exemption and the deliberative process privilege FOIA exemption. Mr. Eddington sued to compel release of the draft report in the US District Court for the District of Columbia. Judge Thomas Penfield Jackson upheld the decision to withhold release of the draft report, agreeing with the claim of the deliberative process privilege. The ATSD(IO) has been advised by counsel for Mr. Eddington that when the MITRE report is finalized, he will file a new FOIA request to obtain the report. Report would not be considered finalized until approved by SECD EF.

92.1 50471

George B. Lofgren II
Assistant to the Secretary Defense
(Intelligence Oversight)

Attachments 7
TABS A-G

Executive Order 12333 - United States Intelligence Activities

Title 3
The President
Presidential Documents
Executive Order 12333 of December 4, 1981
United States Intelligence Activities

Table of Contents

Part 1. Goals, Direction, Duties, and Responsibilities With Respect to the National Intelligence Effort

- 1.1 Goals
- 1.2 The National Security Council
- 1.3 National Foreign Intelligence Advisory Groups
- 1.4 The Intelligence Community
- 1.5 Director Central Intelligence
- 1.6 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies
- 1.7 Senior Officials of the Intelligence Community
- 1.8 The Central Intelligence Agency
- 1.9 The Department of State
- 1.10 The Department of the Treasury
- 1.11 The Department of Defense
- 1.12 Intelligence Components Utilized by the Secretary
- 1.13 The Department of Energy
- 1.14 The Federal Bureau of Investigation

Part 2. Conduct of Intelligence Activities

- 2.1 Need
- 2.2 Purpose
- 2.3 Collection of Information
- 2.4 Collection Techniques
- 2.5 Attorney General Approval
- 2.6 Assistance to Law Enforcement Authorities
- 2.7 Contracting
- 2.8 Consistency With Other Laws
- 2.9 Undisclosed Participation in Organization Within the United States
- 2.10 Human Experimentation
- 2.11 Prohibition on Assassination
- 2.12 Indirect Participation

Part 3. General Provisions

- 3.1 Congressional Oversight
- 3.2 Implementation
- 3.3 Procedure
- 3.4 Definitions
- 3.5 Purpose and Effect
- 3.6 Revocation

Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by virtue of the authority vested in me by the Constitution and statutes of the United States of America, including the National Security Act of 1947, as amended, and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

Part 1.

Goal, Direction, Duties and Responsibilities With Respect to the National Intelligence Effort

1.1 Goals. The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.

(b) 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. A balanced approach between technical collection efforts and other means should be maintained and encouraged.

(c) Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons.

(d) 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.

1.2 The National Security Council.

(a) Purpose. The National Security Council (NSC) was established by the National Security Act of 1947 to advise the President with respect to the integration of domestic, foreign and military policies relating to the national security. The NSC shall act as the highest Executive Branch entity that provides review of, guidance for and direction to the conduct of all national foreign intelligence, counterintelligence, and special activities, and attendant policies and programs.

(b) Committees. The NSC shall establish such committees as may be necessary to carry out its functions and responsibilities under this Order. The NSC or a committee established by it, shall consider and submit to the President a policy recommendation, including all dissents, on each special activity and shall review proposals for other sensitive intelligence operations.

1.3 National Foreign Intelligence Advisory Groups.

(a) Establishment and Duties. The Director of Central Intelligence shall establish such boards, councils... or groups as required for the purpose of obtaining advice from within the Intelligence Community concerning:

- (1) Production, review and coordination of national foreign intelligence;
- (2) Priorities for the National Foreign Intelligence Program budget;
- (3) Interagency exchanges of foreign intelligence information;
- (4) Arrangements with foreign governments on intelligence matters;
- (5) Protection of intelligence sources and methods;
- (6) Activities of common concern; and

(7) Such other matters as may be referred by the Director of Central Intelligence.

(b) Membership. Advisory groups established pursuant to this section

shall be chaired by the Director of Central Intelligence or his designated representative and shall consist of senior representatives from organizations within the Intelligence Community and from departments or agencies containing such organizations, as designated by the Director of Central Intelligence. Groups for consideration of substantive intelligence matters will include representatives of organizations involved in the collection, processing and analysis of intelligence. A senior representative of the Secretary of Commerce, the Attorney General, the Assistant to the President for National Security Affairs, and the Office of the Secretary of Defense shall be invited to participate in any group which deals with other than substantive intelligence matters.

1.4 The Intelligence Community. The agencies within the Intelligence Community shall, in accordance with applicable United States law and with the other provisions of this Order, conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States, including:

(a) Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;

(b) Production and dissemination of intelligence;

(c) Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(d) Special activities;

(e) Administrative and support activities within the United States and abroad necessary for the performance of authorized activities; and

(f) Such other intelligence activities as the President may direct from time to time.

1.5 Director of Central Intelligence

In order to discharge the duties and responsibilities prescribed by law, the Director of Central Intelligence shall be responsible directly to the President and the NSC and shall:

(a) Act as the primary adviser to the President and the NSC on national foreign intelligence and provide the President and other officials in the Executive Branch with national foreign intelligence;

(b) Develop such objectives and guidance for the Intelligence Community as will enhance capabilities for responding to expected future needs for national foreign intelligence;

(c) Promote the development and maintenance of services of common concern by designated intelligence organizations on behalf of the Intelligence Community;

(d) Ensure implementation of special activities;

(e) Formulate policies concerning foreign intelligence and counterintelligence arrangements with foreign governments; coordinate foreign intelligence and counterintelligence relationships between agencies of the Intelligence Community and the intelligence or internal security services of foreign governments, and establish procedures governing the conduct of liaison by any department or agency with such services on narcotics activities;

(f) Participate in the development of procedures approved by the Attorney General governing criminal narcotics intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(g) Ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products;

(h) Ensure that programs are developed which protect intelligence sources, methods, and analytical procedures;

(i) Establish uniform criteria for the determination of relative priorities for the transmission of critical national foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such intelligence;

(j) Establish appropriate staffs, committees, or other advisory groups to assist in the execution of the Director's responsibilities;

(k) Have full responsibility for production and dissemination of national foreign intelligence, and authority to levy analytic tasks on departmental intelligence production organizations, in consultation with those organizations, ensuring that appropriate mechanisms for competitive analysis are developed so that diverse points of view are considered fully and differences of judgment within the Intelligence Community are brought to the attention of national policymakers;

(l) Ensure the timely exploitation - and dissemination of data gathered by national foreign intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government entities and military commands;

(m) Establish mechanisms which translate national foreign intelligence objectives and priorities approved by the NSC into specific guidance for the Intelligence Community, resolve conflicts in tasking priority, provide to departments and agencies having information collection capabilities that are not part of the National Foreign Intelligence Program advisory tasking concerning collection of national foreign intelligence, and provide for the development of plans and arrangements for transfer of required collection tasking authority to the Secretary of Defense when directed by the President;

(n) Develop, with the advice of the program managers and departments and agencies concerned, the consolidated National Foreign Intelligence Program budget, and present it to the President and the Congress;

(o) Review and approve all requests for reprogramming National Foreign Intelligence Program funds, in accordance with guidelines established by the Office of Management and Budget;

(p) Monitor National Foreign Intelligence Program implementation, and, as necessary, conduct program and performance audits and evaluations;

(q) Together with the Secretary of Defense, ensure that there is no unnecessary overlap between national foreign... intelligence programs and Department of Defense intelligence programs consistent with the requirement to develop competitive analysis, and provide to and obtain from the Secretary of Defense all information necessary for this purpose;

(r) In accordance with law and relevant procedures approved by the Attorney General under this Order, give the heads of the departments and agencies access to all intelligence, developed by the CIA or the staff elements of the Director of Central Intelligence, relevant to the national intelligence needs of the departments and agencies; and

(s) Facilitate the use of national foreign intelligence products by Congress in a secure manner.

1.6 Duties Responsibilities of the Heads of Executive Branch Departments and Agencies.

(a) The heads of all Executive Branch departments and agencies shall, in accordance with law and relevant procedures approved by the Attorney General under this Order, give the Director of Central Intelligence access to all information relevant to the national intelligence needs of the United

States, and shall give due consideration to the requests from the Director of Central Intelligence for appropriate support for Intelligence Community activities.

(b) The heads of departments and agencies involved in the National Foreign Intelligence Program shall ensure timely development and submission to the Director of Central Intelligence by the program managers and heads of component activities of proposed national programs and budgets in the format designated by the Director of Central Intelligence, and shall also ensure that the Director of Central Intelligence is provided, in a timely and responsive manner, all information necessary to perform the Director's program and budget responsibilities.

(c) The heads of departments and agencies involved in the National Foreign Intelligence Program may appeal to the President decisions by the Director of Central Intelligence on budget or reprogramming matters of the National Foreign Intelligence Program.

1.7 Senior Officials of the Intelligence Community. The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, as appropriate, shall:

(a) Report to the Attorney General possible violations of federal criminal laws by employees and of specified federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(b) In any case involving serious or continuing breaches of security, recommend to the Attorney General that the case be referred to the FBI for further investigation;

(c) Furnish the Director of Central Intelligence and the NSC, in accordance with applicable law and procedures approved by the Attorney General under this Order, the information required for the performance of their respective duties;

(d) Report to the Intelligence Oversight Board and keep the Director of Central Intelligence appropriately informed, concerning any intelligence activities of their organizations that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive;

(e) Protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the Director of Central Intelligence;

(f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the Director of Central Intelligence;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of intelligence resulting from criminal narcotics intelligence activities abroad if their departments, agencies, or organizations have intelligence responsibilities for foreign or domestic narcotics production and trafficking;

(h) Instruct their employees to cooperate fully with the Intelligence Oversight Board; and

(i) Ensure that the Inspectors General and General Counsels for their organizations have access to any information necessary to perform their duties assigned by this Order.

1.8 The Central Intelligence Agency. All duties and responsibilities of the CIA shall be related to the intelligence functions set out below. As authorized by this Order, the National Security Act of 1947, as amended; the CIA Act of 1949, as amended; appropriate directives or other applicable law, the CIA shall:

(a) Collect, produce and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable.

The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(b) Collect, produce and disseminate intelligence on foreign aspects of narcotics production and trafficking;

(c) Conduct counterintelligence activities outside the United States and, without assuming or performing any internal security functions, conduct counterintelligence activities within the United States in coordination with the FBI as required by procedures agreed upon the Director of Central Intelligence and the Attorney General;

(d) Coordinate counterintelligence activities and the collection of information not otherwise obtainable when conducted outside the United States by other departments and agencies;

(e) Conduct special activities approved by the President. 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;

(f) Conduct services of common concern for the Intelligence Community as directed by the NSC;

(g) Carry out or contract, for research, development and procurement of technical systems and devices relating to authorized functions;

(h) Protect the security of its installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the CIA as are necessary; and

(i) Conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (a) and through (h) above, including procurement and essential cover and proprietary arrangements.

1.9 The Department of State. The Secretary of State shall:

(a) Overtly collect information relevant to United States foreign policy concerns;

(b) Produce and disseminate foreign intelligence relating to United States foreign policy as required for the execution of the Secretary's responsibilities;

(c) Disseminate, as appropriate, reports received from United States diplomatic and consular posts;

(d) Transmit reporting requirements of the Intelligence Community to the Chiefs of United States Missions abroad; and

(e) Support Chiefs of Missions in discharging their statutory responsibilities for direction and coordination of mission activities.

1.10 The Department of the Treasury. The Secretary of the Treasury shall:

(a) Overtly collect foreign financial and monetary information;

(b) Participate with the Department of State in the overt collection of general foreign economic information;

(c) Produce and disseminate foreign intelligence relating to United States economic policy as required for the execution of the Secretary's responsibilities; and

(d) Conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being

used against the President of the United States, the Executive Office of the President, and, as authorized by the Secretary of the Treasury or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against such surveillance, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of the Treasury and the Attorney General.

1.11 The Department of Defense. The Secretary of Defense shall:

(a) Collect national foreign intelligence and be responsive to collection tasking by the Director of Central Intelligence;

(b) Collect, produce and disseminate military and military-related foreign intelligence and counterintelligence as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national departmental and tactical foreign intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components outside the United States in coordination with the CIA, and within the United States in coordination with the FBI pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General;

(e) Conduct, as the executive agent of the United States Government, signals intelligence and communications security activities, except as otherwise directed by the NSC;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director of Central Intelligence, within the United States Government;

(g) Carry out or contract for research, development and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain military intelligence relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations, and ensure that such relationships and programs are in accordance with policies formulated by the Director of Central Intelligence;

(j) Direct, operate, control, and provide fiscal management for the National Security Agency and for defense and military intelligence and national reconnaissance entities; and

(k) Conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (a) through (j) above.

1.12 Intelligence Components Utilized by the Secretary of Defense. In carrying out the responsibilities assigned in section 1.11, the Secretary of Defense is authorized to utilize the following:

(a) Defense Intelligence Agency, whose responsibilities shall include;

(1) Collection, production, or, through tasking and coordination, provision of military and military-related intelligence for the Secretary of Defense, the Joint Chiefs of Staff, other Defense components, and, as appropriate, non-Defense agencies;

(2) Collection and provision of military intelligence for national foreign intelligence and counterintelligence products;

(3) Coordination of all Department of Defense intelligence collection requirements;

(4) Management of the Defense Attache system; and

(5) Provision of foreign intelligence and counterintelligence staff support as directed by the Joint Chiefs of Staff.

(b) National Security Agency whose responsibilities shall include:

(1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense:

(2) Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;

(6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;

(7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence;

(8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;

(9) Conduct of research and development to meet the needs of the United States for signals intelligence and communications security;

(10) Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary;

(11) Prescribing, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;

(12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and

(13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (12) above, including procurement.

(c) Offices for the collection of specialized intelligence through reconnaissance programs, whose responsibilities shall include:

(1) Carrying out consolidated reconnaissance programs for specialized intelligence;

(2) Responding to tasking in accordance with procedures established by the Director of Central Intelligence; and

(3) Delegating authority to the various departments and agencies for research, development, procurement, and operation of designated means of collection.

(d) The foreign intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps, whose responsibilities shall include:

(1) Collection, production and dissemination of military and military-related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics production and trafficking. When collection is conducted in response to national foreign intelligence requirements, it will be conducted in accordance with guidance from the Director of Central Intelligence. Collection of national foreign intelligence, not otherwise obtainable, outside the United States shall be coordinated with the CIA, and such collection within the United States shall be coordinated with the FBI;

(2) Conduct of counterintelligence activities outside the United States coordination with the CIA, and within the United States in coordination with the FBI; and

(3) Monitoring of the development, procurement and management of tactical intelligence systems and equipment and conducting related research, development and test and evaluation activities.

(e) Other offices within the Department of Defense appropriate for conduct of the intelligence missions and responsibilities assigned to the Secretary of Defense. If such other offices are used for intelligence purposes, the provision of Part 2 of this Order shall apply to those offices when used for those purposes

1.13 The Department of Energy. The Secretary of Energy shall:

(a) Participate with the Department of State in overtly collecting information with respect to foreign energy matters;

(b) Produce and disseminate foreign intelligence necessary for the Secretary's responsibilities

(c) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(d) Provide expert technical, analytical and research capability to other agencies within the Intelligence Community

1.14 The Federal Bureau of Investigation. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the FBI shall:

(a) Within the United States conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community. When a counterintelligence activity of the FBI involves military or civilian personnel of the Department of Defense, the FBI shall coordinate with the Department of Defense;

(b) Conduct counterintelligence activities outside the United States in coordination with the CIA as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(c) Conduct within the United States, when requested by officials of

the Intelligence Community designated by the President, activities undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the Intelligence Community, or, when requested by the Director of the National Security Agency, to support the communications security activities of the United States Government;

(d) Produce and disseminate foreign intelligence and counterintelligence; and

(e) Carry out or contract for research, development and procurement of technical systems and devices relating to the functions authorized above

Part 2

Conduct of Intelligence Activities

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

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

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

(a) Information that is publicly available or collected with the consent of the person concerned;

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

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

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

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

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

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

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

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

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

2.4 Collection Techniques. Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, 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. These procedures shall not authorize:

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

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

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

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

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

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

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

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

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

accordance with that Act, as well as this Order.

2.6 Assistance to Law Enforcement Authorities. Agencies within the Intelligence Community are authorized to:

- (a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community;
- (b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
- (c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency; and
- (d) Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

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

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes or United States.

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

- (a) The participation is undertaken on behalf of the FBI in the course of lawful investigation; or
- (b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign Power.

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

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

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

Part 3

General Provisions

3.1 Congressional Oversight The duties and responsibilities of the Director of Central Intelligence and the heads of other departments,

agencies, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be as provided in title 50, United States Code, section 413. The requirements of section 662 of the Foreign Assistance Act of 1961, as amended (22 U.S.C. 222), and section 501 of the National Security Act of 1947, as amended (50 U.S.C. 413) shall apply to all special activities as defined in this Order.

3.2 Implementation. The NSC, the Secretary of Defense, the Attorney General, and the Director of Central Intelligence shall issue such appropriate directives and Procedures as are necessary to implement this Order. Heads of agencies within the Intelligence Community shall issue appropriate supplementary directives and procedures consistent with this Order. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an agency in the Intelligence Community other than the FBI. The National Security Council may establish procedures in instances where the agency head and the Attorney General are unable to reach agreement on other than constitutional or other legal grounds.

3.3 Procedures. Until the procedures required by this Order have been established, the activities herein authorized which require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order No. 12036. Procedures required by this Order shall be established as expeditiously as possible. All procedures promulgated pursuant to this Order shall be made available to the congressional intelligence committees.

3.4 Definitions. For the purposes of this Order, the following terms shall have these meanings:

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

(b) Electronic surveillance means 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 communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(c) Employee means a person employed by, assigned to or acting for an agency within the Intelligence Community.

(d) Foreign intelligence means information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

(e) Intelligence activities means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to this Order.

(f) Intelligence Community and agencies within the Intelligence Community refer to the following agencies or organizations:

- (1) The Central Intelligence Agency (CIA);
- (2) The National Security Agency (NSA);
- (3) The Defense Intelligence Agency (DIA);
- (4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
- (5) The Bureau of Intelligence and Research of the Department of State;
- (6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the

Treasury, and the Department of Energy; and

(7) The staff elements of the Director of Central Intelligence.

(g) The National Foreign Intelligence Program includes the programs listed below, but its composition shall be subject to review by the National Security Council and modification by the President:

(1) The programs of the CIA;

(2) The Consolidated Cryptologic Program, the General Defense Intelligence Program, and the programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance, except such elements as the Director of Central Intelligence and the Secretary of Defense agree should be excluded;

(3) Other programs of agencies within the Intelligence Community designated jointly by the Director of Central Intelligence and the head of the department or by the President as national foreign intelligence or counterintelligence activities;

(4) Activities of the staff elements of the Director of Central Intelligence;

(5) Activities to acquire the intelligence required for the planning and conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program.

(h) Special activities means activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions.

(i) United States person means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments

3.5 Purpose and Effect. This Order is intended to control and provide direction and guidance to the Intelligence Community. Nothing contained herein or in any procedures promulgated hereunder is intended to confer any substantive or procedural right or privilege on any person or organization....

3.6 Revocation. Executive Order No. 12036 of January 24, 1978, as amended, entitled "United States Intelligence Activities," is revoked.

THE WHITE HOUSE,
December 4, 1981.





DEPARTMENT OF DEFENSE

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

DECEMBER 1982

UNDER SECRETARY OF DEFENSE FOR POLICY


PREFACE

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

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

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

This regulation is effective immediately.

 10/4/82
Attorney General of the
United States

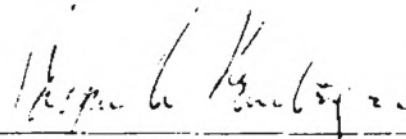
 12/7/82
Secretary of Defense

TABLE OF CONTENTS

	<u>Page</u>
Foreword	i
Table of Contents	ii
References	vii
 PROCEDURE 1. GENERAL PROVISIONS	 1-1
A. Applicability and Scope	1-1
B. Purpose	1-1
C. Interpretation	1-1
D. Exceptions to Policy	1-2
E. Amendment	1-2
 PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS	 2-1
A. Applicability and Scope	2-1
B. Explanation of Undefined Terms	2-1
C. Types of Information That May be Collected About United States Persons	2-1
1. Information obtained with consent	2-1
2. Publicly-available information	2-1
3. Foreign intelligence	2-1
4. Counterintelligence	2-2
5. Potential sources of assistance to intelligence activities	2-2
6. Protection of intelligence sources and methods	2-2
7. Physical security	2-3
8. Personnel security	2-3
9. Communications security	2-3
0. Narcotics	2-3
1. Threats to safety	2-3
2. Overhead reconnaissance	2-3
3. Administrative purpose	2-3
D. General Criteria Governing the Means Used to Collect Information About United States Persons	2-3
1. Means of collection	2-3
2. Least intrusive means	2-3
E. Special Limitation on the Collection of Foreign Intelligence Within the United States	2-4
 PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS	 3-1
A. Applicability	3-1
B. Explanation of Undefined Terms	3-1

C.	Criteria for Retention	3-1
1.	Retention of information collected under Procedure 2	3-1
2.	Retention of information acquired incidentally	3-1
3.	Retention of information relating to functions of other DoD Components or non-DoD Agencies	3-1
4.	Temporary retention	3-1
5.	Retention of other information	3-1
D.	Access and Retention	
1.	Controls on access to retained information	3-2
2.	Duration of retention	3-2
3.	Information acquired prior to effective date	3-2
PROCEDURE 4.	DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS	4-1
A.	Applicability and Scope	4-1
B.	Criteria for Dissemination	4-1
C.	Other Dissemination	4-1
PROCEDURE 5.	ELECTRONIC SURVEILLANCE	5-1
Part 1.	Electronic Surveillance in the United States for Intelligence Purposes	5-1
A.	Applicability	5-1
B.	General Rules	5-1
1.	Electronic surveillance pursuant to the Foreign Intelligence Surveillance Act	5-1
2.	Authority to request electronic surveillance	5-1
3.	Electronic surveillance in emergency situations	5-1
Part 2.	Electronic Surveillance Outside the United States for Intelligence Purposes	5-2
A.	Applicability	5-2
B.	Explanation of Undefined Terms	5-2
C.	Procedures	5-2
D.	Electronic Surveillance in Emergency Situations	5-3
E.	Officials Authorized to Request and Approve Electronic Surveillance Outside the United States	5-4

Part 3.	Signals Intelligence Activities	
A.	Applicability and Scope	5-5
B.	Explanation of Undefined Terms	5-5
C.	Procedures	5-6
1.	Foreign communications	5-6
2.	Military tactical communications	5-6
Part 4.	Technical Surveillance Countermeasures	5-8
A.	Applicability and Scope	5-8
B.	Explanation of Undefined Terms	5-8
C.	Procedures	5-8
Part 5.	Developing, Testing and Calibration of Electronic Equipment	5-9
A.	Applicability	5-9
B.	Procedures	5-9
1.	Signals authorized for use	5-9
2.	Restrictions	5-10
Part 6.	Training of Personnel in the Operation and Use of Electronic Communications and Surveillance Equipment	5-11
A.	Applicability	5-11
B.	Procedures	5-11
1.	Training guidance	5-11
2.	Training limitations	5-11
3.	Retention and dissemination	5-12
Part 7.	Conduct of Vulnerability and Hearability Surveys	5-13
A.	Applicability and Scope	5-13
B.	Explanation of Undefined Terms	5-13
C.	Procedures	5-13
1.	Conduct of vulnerability surveys	5-13
2.	Conduct of hearability surveys	5-13
PROCEDURE 6.	CONCEALED MONITORING	6-1
A.	Applicability and Scope	6-1
B.	Explanation of Undefined Terms	6-1
C.	Procedures	6-2
PROCEDURE 7.	PHYSICAL SEARCHES	7-1
A.	Applicability	7-1
B.	Explanation of Undefined Terms	7-1
C.	Procedures	7-1
1.	Unconsented physical searches within the United States	7-1
2.	Unconsented physical searches outside the United States	7-1

PROCEDURE 8.	SEARCHES AND EXAMINATION OF MAIL	8-1
A.	Applicability	8-1
B.	Explanation of Undefined Terms	8-1
C.	Procedures	8-1
	1. Searches of mail within United States postal channels	8-1
	2. Searches of mail outside United States postal channels	8-2
	3. Mail Covers	8-2
PROCEDURE 9.	PHYSICAL SURVEILLANCE	9-1
A.	Applicability	9-1
B.	Procedures	9-1
	1. Criteria for physical surveillance in the United States	9-1
	2. Criteria for physical surveillance outside the United States	9-1
	3. Required approvals for physical surveillance	9-1
PROCEDURE 10.	UNDISCLOSED PARTICIPATION IN ORGANIZATIONS	10-1
A.	Applicability	10-1
B.	Explanation of Undefined Terms	10-1
C.	Procedures for Undisclosed Participation	10-2
	1. Limitations on Undisclosed Participation	10-2
	2. Required Approvals	10-2
D.	Disclosure Requirement	10-4
PROCEDURE 11.	CONTRACTING FOR GOODS AND SERVICES	11-1
A.	Applicability	11-1
B.	Procedures	11-1
	1. Contracts with academic institutions	11-1
	2. Contracts with commercial organizations, private institutions, and individuals	11-1
C.	Effect of Noncompliance	11-1
PROCEDURE 12.	PROVISIONS OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES	12-1
A.	Applicability	12-1
B.	Procedures	12-1
	1. Cooperation with law enforcement authorities	12-1
	2. Types of permissible assistance	12-1

PROCEDURE 13.	EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES	13-1
A.	Applicability	13-1
B.	Explanation of Undefined Terms	13-1
C.	Procedures	13-1
PROCEDURE 14.	EMPLOYEE CONDUCT	14-1
A.	Applicability	14-1
B.	Procedures	14-1
1.	Employee responsibility	14-1
2.	Familiarity with restrictions	14-1
3.	Responsibilities of the heads of DoD Components	14-1
PROCEDURE 15.	IDENTIFYING, INVESTIGATING AND REPORTING QUESTIONABLE ACTIVITIES	15-1
A.	Applicability	15-1
B.	Explanation of Undefined Terms	15-1
C.	Procedures	15-1
1.	Identification	15-1
2.	Investigation	15-2
3.	Reports	15-2
Appendix A -	Definitions	A-1

REFERENCES

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

PROCEDURE 1. GENERAL PROVISIONS

A. APPLICABILITY AND SCOPE

1. These procedures apply only to "DoD intelligence components," as defined in Appendix A. Procedures 2 through 4 provide the sole authority by which such components may collect, retain and disseminate information concerning United States persons. Procedures 5 through 10 set forth applicable guidance with respect to the use of certain collection techniques to obtain information for foreign intelligence and counterintelligence purposes. Authority to employ such techniques shall be limited to that necessary to perform functions assigned the DoD intelligence component concerned. Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities.

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

3. These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcement procedures.

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

B. PURPOSE

The purpose of these procedures is to enable DoD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

C. INTERPRETATION

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

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

3. All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned. Questions that cannot be resolved in this manner shall be referred to the General Counsel of the Military Department concerned, or, as appropriate, the General Counsel of the Department of Defense for resolution.

D. EXCEPTIONS TO POLICY

Requests for exception to the policies and procedures established herein shall be made in writing to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense and, if required, the Attorney General for any such exception.

E. AMENDMENT

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

PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

A. APPLICABILITY AND SCOPE

This procedure specifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information. Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques.

B. EXPLANATION OF UNDEFINED TERMS

1. Collection. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

2. Cooperating sources means persons or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information at the request of such components or on their own initiative. These include government agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments.

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

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

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

Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:

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

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

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

- 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 victims of international terrorist organizations; or
- e. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

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

- a. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.
- b. Persons in contact with persons described in paragraph C.4.a., above, for the purpose of identifying such person and assessing their relationship with persons described in paragraph C.4.a., above.

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

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

- a. Present and former DoD employees;

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

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

7. Physical security. Information may be collected about a United States person who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors. Information may also be collected in the course of a lawful physical security investigation.

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

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

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

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

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

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

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

1. Means of collection. DoD intelligence components are authorized to collect information about United States persons by any lawful means, provided that all such collection activities shall be carried out in accordance with E.O. 12333 (reference (a)), and this Regulation, as appropriate.

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

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

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

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

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

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

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

1. The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any United States person;
2. Such foreign intelligence cannot be reasonably obtained by overt means;
3. The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI); and
4. The use of other than overt means has been approved in writing by the head of the DoD intelligence component concerned, or his single designee, as being consistent with these procedures. A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy).

PROCEDURE 3 RETENTION OF INFORMATION
ABOUT UNITED STATES PERSONS

A. APPLICABILITY

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

B. EXPLANATION OF UNDEFINED TERMS

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.

C. CRITERIA FOR RETENTION

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

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

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

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

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

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

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

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

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

D. ACCESS AND RETENTION

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

2. Duration of retention. Disposition of information about United States persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained.

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

PROCEDURE 4. DISSEMINATION OF INFORMATION
ABOUT UNITED STATES PERSONS

A. APPLICABILITY AND SCOPE

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

B. CRITERIA FOR DISSEMINATION

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

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

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

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

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

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

d. An agency of the federal government authorized to receive such information in the performance of a lawful governmental function; or

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

C. OTHER DISSEMINATION

Any dissemination that does not conform to the conditions set forth in section B., above, must be approved by the legal office responsible for advising the DoD Component concerned after consultation with the Department of Justice and General Counsel of the Department of Defense. Such approval shall be based on a determination that the proposed dissemination complies with applicable laws, executive orders, and regulations.

PROCEDURE 5. ELECTRONIC SURVEILLANCE

PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSESA. APPLICABILITY

This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

B. GENERAL RULES

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

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

3. Electronic surveillance in emergency situations.

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

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

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

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

A. APPLICABILITY

This part of Procedure 5 applies to electronic surveillance, as defined in Appendix A, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 and the regulation of "signals intelligence activities" under Part 3, so that the intentional interception for foreign intelligence and counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts. In addition, this part governs the use of electronic, mechanical, or other surveillance devices for foreign intelligence and counterintelligence purposes against a United States person abroad in circumstances where such person has a reasonable expectation of privacy. This part does not apply to the electronic surveillance of communications of other than United States persons abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

B. EXPLANATION OF UNDEFINED TERMS

1. Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person. Electronic surveillance directed against persons who are not United States persons that results in the incidental acquisition of the communications of a United States person does not thereby become electronic surveillance directed against a United States person.

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

C. PROCEDURES

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

1. An identification or description of the target.

2. A statement of the facts supporting a finding that:

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

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

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

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

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

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

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

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

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

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

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

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

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

D. ELECTRONIC SURVEILLANCE IN EMERGENCY SITUATIONS

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

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

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

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

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

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

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

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

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

1. The following officials may request approval of electronic surveillance outside the United States under section C., above, and approve emergency surveillance under section D., above:

a. The Secretary and Deputy Secretary of Defense.

b. The Secretaries and Under Secretaries of the Military Departments.

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

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

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

b. The Deputy Director for Operations, National Security Agency.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 3: SIGNALS INTELLIGENCE ACTIVITIESA. APPLICABILITY AND SCOPE

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

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

B. EXPLANATION OF UNDEFINED TERMS

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

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

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

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

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

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

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

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

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

C. PROCEDURES

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

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

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

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

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

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continuedPART 4: TECHNICAL SURVEILLANCE COUNTERMEASURESA. APPLICABILITY AND SCOPE

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

B. EXPLANATION OF UNDEFINED TERMS

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

C. PROCEDURES

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

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

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

3. Access to the content of communications acquired during the use of countermeasures is limited to persons involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use. However, if the content is acquired within the United States, only information which is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (c)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated only for these purposes. If acquired outside the United States, information which indicates a violation of federal law including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities. A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained.

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 5: DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENTA. APPLICABILITY

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

B. PROCEDURES1. Signals authorized for use.a. The following may be used without restriction:

- (1) Laboratory-generated signals.
- (2) Communications signals with the consent of the communicator.
- (3) Communications in the commercial or public service broadcast bands.

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

(5) Noncommunications signals (including telemetry, and radar).

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

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

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

(2) Communications in the citizens and amateur-radio bands.

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

2. Restrictions.

For signals described in paragraph B.1.c. and d., above, the following restrictions apply:

a. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in section A., above.

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

c. The content of any communication shall:

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

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

(3) Be destroyed immediately upon completion of the activity.

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

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 6. TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENTA. APPLICABILITY

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

B. PROCEDURES

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

2. Training limitations

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

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

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

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

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

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

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

PROCEDURE 5. ELECTRONIC SURVEILLANCE, continued

PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYSA. APPLICABILITY AND SCOPE

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

B. EXPLANATION OF UNDEFINED TERMS

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

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

C. PROCEDURES

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

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

b. No transmission may be acquired aurally.

c. No content of any transmission may be acquired by any means.

d. No transmissions may be recorded.

e. No report or log may identify any United States person or entity except to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

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

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

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

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

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

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

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

PROCEDURE 6. CONCEALED MONITORING

A. APPLICABILITY AND SCOPE

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

2. Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure.

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

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

B. EXPLANATION OF UNDEFINED TERMS

1. Concealed monitoring means targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time.

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

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

C. PROCEDURES

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

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

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

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

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

PROCEDURE 7. PHYSICAL SEARCHES

A. APPLICABILITY

This procedure applies to unconsented physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes. DoD intelligence components may provide assistance to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12.

B. EXPLANATION OF UNDEFINED TERMS

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

C. PROCEDURES1. Unconsented physical searches within the United States.

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

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

2. Unconsented physical searches outside the United States.

a. Searches of active duty military personnel for counterintelligence purposes. The counterintelligence elements of the Military Departments may conduct unconsented physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes

when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C.2.B.(2), below.

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

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

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

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

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

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

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

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

(3) A statement of facts 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.

c. Requests for approval of unconsented physical searches under paragraph C.2.1. 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.

PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

A. APPLICABILITY

This procedure applies to the opening of mail in United States postal channels, and the use of mail covers with respect to such mail, for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from United States persons where such activity is conducted outside the United States and such mail is not in United States postal channels.

B. EXPLANATION OF UNDEFINED TERMS

1. Mail within United States postal channels includes:

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

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

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

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

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

C. PROCEDURES

1. Searches of mail within United States postal channels.

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

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

in accordance with applicable postal regulations. Such components may also request appropriate U.S. postal authorities to detain, or permit the detention of, mail that may become subject to search under this section, in accordance with applicable postal regulations.

2. Searches of mail outside United States postal channels.

a. DoD intelligence components are authorized to open mail to or from a United States person that is found outside United States postal channels only pursuant to the approval of the Attorney General. Requests for such approval shall be treated as a request for an unconsented physical search under paragraph C.2.b. of Procedure 7.

b. Heads of DoD intelligence components may authorize the opening of mail outside U.S. postal channels when both the sender and intended recipient are other than United States persons if such searches are otherwise lawful and consistent with any Status of Forces Agreement that may be in effect.

3. Mail covers

a. DoD intelligence components may request U.S. postal authorities to examine mail in U.S. postal channels, for counterintelligence purposes, in accordance with applicable postal regulations.

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

PROCEDURE 9. PHYSICAL SURVEILLANCE

A. APPLICABILITY

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

B. EXPLANATION OF UNDEFINED TERMS

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

C. PROCEDURES

1. Criteria for physical surveillance in the United States. Within the United States, DoD intelligence components may conduct unconsented physical surveillances for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence component concerned; present or former contractors of such components or their present or former employees; applicants for such employment or contracting; or military persons employed by a nonintelligence element of a Military Service. Any physical surveillance within the United States that occurs outside a DoD installation shall be coordinated with the FBI and other law enforcement agencies as may be appropriate.

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

3. Required approvals for physical surveillance.

a. Persons within DoD investigative jurisdiction. Physical surveillances within the United States or which involve United States persons within DoD investigative jurisdiction overseas may be approved by the head of the DoD intelligence component concerned or by designated senior officials of such components in accordance with this procedure.

b. Persons outside DoD investigative jurisdiction. Outside the United States, physical surveillances of United States persons who are not within the investigative jurisdiction of the DoD intelligence component concerned will be forwarded through appropriate channels to the Deputy Under Secretary of Defense (Policy) for approval. Such requests shall indicate coordination with the Central Intelligence Agency.

PROCEDURE 10 UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

A. APPLICABILITY

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

B. EXPLANATION OF UNDEFINED TERMS

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

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

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

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

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

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

C. PROCEDURES FOR UNDISCLOSED PARTICIPATION

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

1. Limitations on undisclosed participation.

a. Lawful purpose. No undisclosed participation shall be permitted under this procedure unless it is essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of the collecting DoD intelligence component.

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

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

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

2. Required Approvals

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

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

(2) Participation in organizations that permit other persons acknowledged to the organization to be employees of the U.S. Government to participate.

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

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

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

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

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

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

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

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

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

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

D. DISCLOSURE REQUIREMENT

1. Disclosure of the intelligence affiliation of an employee of a DoD intelligence component shall be made to an executive officer of the organization in question, or to an official in charge of membership, attendance or the records of the organization concerned.

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

PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES

A. APPLICABILITY

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

B. PROCEDURES

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

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

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

b. There is a written determination by the Secretary or the Under Secretary of a Military Department, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, or the Deputy Under Secretary of Defense (Policy) that the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned.

C. EFFECT OF NONCOMPLIANCE

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

PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES

A. APPLICABILITY

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

B. PROCEDURES

1. Cooperation with law enforcement authorities. Consistent with the limitations contained in DoD Directive 5525.5 (reference (i)), and subsection B.2., below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:

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

b. Protecting DoD employees, information, property, and facilities;
and

c. Preventing, detecting, or investigating other violations of law.

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

a. Incidentally-acquired information reasonably believed to indicate a violation of federal law shall be provided in accordance with the procedures adopted pursuant to section 1.7 (a) of E.O. 12333 (reference (a));

b. Incidentally-acquired information reasonably believed to indicate a violation of state, local, or foreign law may be provided in accordance with procedures adopted by the heads of DoD Components;

c. Specialized equipment and facilities may be provided to federal law enforcement authorities, and, when lives are endangered, to state and local law enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to, enclosure 3 of DoD Directive 5525.5 (reference (i)); and

d. Personnel who are employees of DoD intelligence components may be assigned to assist federal law enforcement authorities, and, when lives are endangered, state and local law enforcement authorities, provided such use is consistent with, and has been approved by an official authorized pursuant to, enclosure 4 of DoD Directive 5525.5 (reference (i)). Such official shall ensure that the General Counsel of the providing DoD Component concurs in such use.

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

PROCEDURE 13 EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

A. APPLICABILITY

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

B. EXPLANATION OF UNDEFINED TERMS

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

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

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

C. PROCEDURES

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

2. DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the Secretary or Deputy Secretary of Defense, or the Secretary or Under Secretary of a Military Department, as appropriate.

PROCEDURE 14. EMPLOYEE CONDUCT

A. APPLICABILITY

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

B. PROCEDURES

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

2. Familiarity with restrictions.

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

- (1) Applicable portions of Procedures 1 through 4;
- (2) A summary of other procedures that pertains to collection techniques which are, or may be, employed by the DoD intelligence component concerned; and
- (3) A statement of individual employee reporting responsibility under Procedure 15.

b. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(10)) and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect which will achieve the objectives set forth in paragraph B.2.a., above.

3. Responsibilities of the heads of DoD Components. The heads of DoD Components that constitute, or contain, DoD intelligence components shall:

- a. Ensure that all proposals for intelligence activities which may be unlawful, in whole or in part, or may be contrary to applicable Executive Branch or DoD policy are referred to the General Counsel responsible for such component.
- b. Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15.
- c. Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder.

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

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

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

PROCEDURE 15. IDENTIFYING, INVESTIGATING,
AND REPORTING QUESTIONABLE ACTIVITIES

A. APPLICABILITY

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

B. EXPLANATION OF UNDEFINED TERMS

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

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

C. PROCEDURES

1. Identification.

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

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

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

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

2. Investigation.

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

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

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

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

3. Reports.

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

b. Each General Counsel and Inspector General shall submit to the ATSD(IO) a quarterly report describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive Order or Presidential directive, or applicable DoD policy; and actions taken with respect to such activities. The reports shall also include significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system. Separate, joint, or consolidated reports may be submitted. These reports should be prepared in accordance with DoD Directive 5000.11 (reference (j)).

c. All reports made pursuant to paragraph C.3.a. and b., above, which involve a possible violation of federal criminal law shall be considered by the General Counsel concerned in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a)).

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

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

f. These reporting requirements are exempt from formal approval and licensing in accordance with subsection VII.G. of enclosure 3 to DoD Directive 5000.19 (reference (k)).

APPENDIX A

DEFINITIONS

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

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

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

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

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

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

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

8. DoD intelligence components. Include the following organizations:
- a. The National Security Agency, Central Security Service.
 - b. The Defense Intelligence Agency.
 - c. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
 - d. The Assistant Chief of Staff for Intelligence, Army General Staff.
 - e. The Office of Naval Intelligence.
 - f. The Assistant Chief of Staff, Intelligence, U.S. Air Force.
 - g. The Army Intelligence and Security Command.
 - h. The Naval Intelligence Command.
 - i. The Naval Security Group Command.
 - j. The Director of Intelligence, U.S. Marine Corps.
 - k. The Air Force Intelligence Service.
 - l. The Electronic Security Command, U.S. Air Force.
 - m. The counterintelligence elements of the Naval Investigative Service.
 - n. The counterintelligence elements of the Air Force Office of Special Investigations.
 - o. The 650th Military Intelligence Group, SHAPE.
 - p. Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

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

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

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

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

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

14. Intelligence community and an agency of or within the intelligence community. Refers to the following organizations:

- a. The Central Intelligence Agency (CIA).
- b. The National Security Agency (NSA).
- c. The Defense Intelligence Agency (DIA).
- d. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- e. The Bureau of Intelligence and Research of the Department of State.
- f. The intelligence elements of the Army, Navy, Air Force and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.
- g. The staff elements of the Office of the Director of Central Intelligence.

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

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

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

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

19. Personnel security investigation:

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

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

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

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

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

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

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

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

25. United States person.

a. The term "United States person" means:

- (1) A United States citizen;
- (2) An alien known by the DoD intelligence component concerned to be a permanent resident alien;
- (3) An unincorporated association substantially composed of United States citizens or permanent resident aliens;
- (4) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.

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

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



Department of Defense D I R E C T I V E

July 1, 1994
NUMBER 5148.11

DA&M

SUBJECT: Assistant to the Secretary of Defense for Intelligence Oversight
(ATSI(10))

- References:
- (a) Title 10, United States Code
 - (b) DoD Directive 5148.11, "Assistant to the Secretary of Defense (Intelligence Oversight)," December 1, 1982 (hereby canceled)
 - (c) Executive Order 12333, "United States Intelligence Activities," December 1, 1981
 - (d) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1983
 - (e) through (k), see enclosure 1

A. REISSUANCE AND PURPOSE

Under the authority vested in the Secretary of Defense by Section 113 of reference (a), this Directive reissues reference (b) to update the responsibilities, functions, relationships, and authorities of the ATSD(10), as prescribed herein.

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components")

C. DEFINITION

Propriety. Refers to the standards for intelligence activities promulgated in Executive orders, Presidential Directives, and DoD Directives. Other terms used herein are defined in references (c), (d), and (e).

D. RESPONSIBILITIES AND FUNCTIONS

The Assistant to the Secretary of Defense for Intelligence Oversight shall be responsible for the independent oversight of all intelligence activities in the Department of Defense. In this capacity, the ATSD(10) shall ensure that all activities performed by intelligence units and all intelligence activities performed by non-intelligence units, are conducted in compliance with Federal law and other laws as appropriate, Executive orders and Presidential Directives, and DoD Directives System issuances. In the exercise of this responsibility, the ATSD(10) shall:

1. Develop intelligence oversight policy and, in coordination with the General Counsel of the Department of Defense (GC, DoD), issue intelligence oversight guidance to the DoD intelligence components, including regulatory guidance implementing intelligence oversight aspects of E.O. 12333 (reference (c)).

2. Review, in consultation with the GC, DoD, all allegations that raise questions of the legality or propriety of intelligence activities in the Department of Defense.

3. Investigate intelligence activities that raise questions of legality or propriety.

4. Conduct vigorous and independent inspections of the DoD Components that engage in intelligence activities for the purpose of verifying that personnel are familiar and in compliance with E.O. 12333 (reference (c)) and its DoD implementing documents. At the request of senior leadership of the Department, and as practicable, the ATSD(IO) will assess and evaluate the performance of DoD's intelligence activities during the course of scheduled inspections and site visits. Reports in these areas of special interest will be provided to the requesting official and the Secretary of Defense for information.

5. Monitor investigations and inspections conducted by the DoD Components related to intelligence activities, evaluate the findings and, if appropriate, submit recommendations for corrective action to the Secretary and Deputy Secretary of Defense.

6. Report the following to the Secretary and Deputy Secretary of Defense, and the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board, established under E.O. 12863 (reference (f)), at least quarterly, in consultation with the GC, DoD:

a. Any significant oversight activities undertaken; and

b. Any DoD intelligence activities of questionable legality or propriety, the investigative action on them, an evaluation of completed investigations, and the action taken on completed investigations.

7. Participate as a member of the Defense Counterintelligence Board (DoD Directive 5240.2, reference (g)).

8. Pursuant to DoD Directive 5240.12 (reference (h)), review and conduct an annual financial audit of all funds generated by DoD Intelligence Commercial Activities, and report the results to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.

9. Review DoD clandestine intelligence activities to ensure compliance with special constraints and controls.

10. Evaluate the effectiveness of the DoD intelligence components' efforts to protect HUMINT sources, in accordance with DoD Directive S-5205.1 (reference (i)).

11. Participate in the Sensitive Reconnaissance Operations approval process.

12. Conduct liaison with Federal intelligence and law enforcement agencies (e.g., Central Intelligence Agency, Federal Bureau of Investigation, and Drug Enforcement Administration) at the national level and field locations, as required, to ensure DoD intelligence activities and DoD intelligence support to law enforcement agencies are being conducted properly.

13. Review the DoD sensitive support provided to the DoD Components and other Federal Agencies, pursuant to DoD Directive S-5210.36 (reference (j)), to ensure compliance with DoD policy.

14. Coordinate, as appropriate, with the DoD Inspector General (DoD IG) on matters relating to the DoD IG's area of responsibility in accordance with DoD Directive 5106.1 (reference (k)).

15. Perform such other functions as the Secretary of Defense may prescribe.

E. RELATIONSHIPS

1. In the performance of assigned responsibilities and functions, the ATSD(IO) shall serve under the authority, direction, and control of the Secretary of Defense, and shall:

a. Report directly to the Secretary and Deputy Secretary of Defense.

b. Coordinate and exchange information with other OSD officials, heads of the DoD Components, and other Federal officials having collateral or related functions.

c. Use existing facilities and services of the Department of Defense and other Federal Agencies, when practicable, to avoid duplication and to achieve maximum efficiency and economy.

2. Other OSD officials and heads of the DoD Components shall coordinate with the ATSD(IO) on all matters related to the responsibilities and functions cited in section D., above.

F. AUTHORITIES

The ATSD(IO) is hereby delegated authority to:

1. Obtain reports, information, advice, and assistance, consistent with DoD Directive 8910.1 (reference (1)), as necessary, in carrying out assigned functions.

2. Communicate directly with the heads of the DoD Components and, with notification to the Chairman of the Joint Chiefs of Staff, to the Commanders of the Unified Combatant Commands, as necessary, in carrying out assigned functions.

3. Request such temporary assistance from the DoD Components as may be required for the conduct of inspections or investigations, to include personnel.

facilities, and other services. Requests for needed support shall be made in accordance with established procedures.

4. Communicate directly with the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board, the Director of Central Intelligence, other Federal officials, representatives of the legislative branch, members of the public, and representatives of foreign governments, as appropriate, in carrying out assigned functions.

5. Have complete and unrestricted access to all available intelligence-related information, regardless of classification or compartmentation, from all DoD Components and personnel, as required, in carrying out assigned functions. This includes specifically the authority to:

(a) Require an Inspector General or other cognizant investigative official of a DoD Component to report allegations of improprieties or illegalities of intelligence activities by, or within, a DoD Component; and

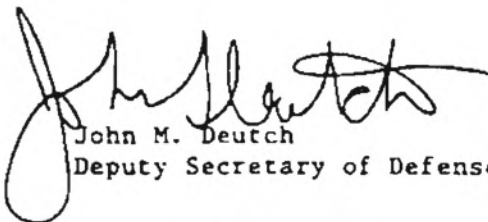
(b) Obtain information on the status, proceedings, and findings or to obtain copies of reports of investigations or inspections of such allegations.

6. Deal directly with the head of the element inspected or investigated, conduct interviews, take depositions, and examine records incident to an inspection or investigation of any DoD Component, as required, in carrying out assigned functions.

G. EFFECTIVE DATE

This Directive is effective immediately.

Enclosure
References


John M. Deutch
Deputy Secretary of Defense

~~FOR OFFICIAL USE ONLY~~

ATSD(IO) Review of NSA Activities - ECHELON ~~(FOUO)~~

~~(FOUO)~~ Early in 2000, the ATSD(IO) began an Intelligence Oversight review of NSA operations in response to media speculation and public discussion about NSA activities the media called "ECHELON." The media speculation included allegations that, through this program NSA violated the rights of United States persons, provided intelligence to U.S. companies to aid them in competing with foreign companies, and used its allies to collect intelligence that was illegal for the U.S. to collect. (Executive Order 12333 and implementing DoD regulations govern the conduct of NSA's activities.)

~~(FOUO)~~ The ATSD(IO) review began with several sessions held at NSA Headquarters at Fort Meade, MD, in which technical, legal, and oversight issues regarding NSA's activities were addressed. The NSA General Counsel, Inspector General, and senior members of their staffs participated, as did personnel from NSA who were directly involved in operations. The ATSD(IO) then personally visited several field locations to continue the review. Once activities were reviewed in the field, the ATSD(IO) team returned to NSA Headquarters to observe and monitor activities there.

~~(FOUO)~~ This review determined that NSA's activities are conducted in compliance with the law and with Executive Order 12333, "United States Intelligence Activities;" DoD 5240.1-F (Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons); and associated NSA Directives. The review further concluded that allegations that our allies are performing intelligence missions which are illegal for the U.S. to perform, and providing the information to the U.S., are groundless. The review also determined there were no indications that NSA provides intelligence information to U.S. companies to assist them in competing with foreign companies.

~~(FOUO)~~ Importantly, the review found that within the NSA workforce there is a strong culture and determination to protect the rights of U.S. persons and conduct activities fully in accordance with the law and governing DoD directives. NSA personnel involved in these operations receive periodic training regarding the relevant laws and rules. There is a significant oversight mechanism in place to ensure that operations are legal and proper and that inadvertent collection of U.S. person information is properly and promptly reported. Oversight and audits of operations are performed internally by NSA personnel as a regular workday procedure. Vigorous oversight is performed internally by the NSA Office of the General Counsel, and the NSA Office of the Inspector General, and externally by the ATSD(IO), the President's Intelligence Oversight Board, the House Permanent Select Committee on Intelligence, and the Senate Select Committee on Intelligence. There are open and frequent communications among operations personnel and oversight and legal experts to address complex Intelligence Oversight issues that arise during the course of operations.

~~FOR OFFICIAL USE ONLY~~

Executive Order 12863

President's Foreign Intelligence Advisory Board

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the security of the United States by improving the quality and effectiveness of intelligence available to the United States, and to assure the legality of activities of the Intelligence Community, it is ordered as follows:

Part I. Assessment of Intelligence Activities

Section 1.1. There is hereby established within the White House Office, Executive Office of the President, the President's Foreign Intelligence Advisory Board (PFIAB). The PFIAB shall consist of not more than 16 members, who shall serve at the pleasure of the President and shall be appointed by the President from among trustworthy and distinguished citizens outside the Government who are qualified on the basis of achievement, experience and independence. The President shall establish the terms of the members upon their appointment. To the extent practicable one-third of the PFIAB at any one time shall be comprised of members whose term of service does not exceed 2 years. The President shall designate a Chairman and Vice Chairman from among the members. The PFIAB shall utilize full-time staff and consultants as authorized by the President. Such staff shall be headed by an Executive Director, appointed by the President.

Sec. 1.2. The PFIAB shall assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, and of counterintelligence and other intelligence activities. The PFIAB shall have the authority to review continually the performance of all agencies of the Federal Government that are engaged in the collection, evaluation, or production of intelligence or the execution of intelligence policy. The PFIAB shall further be authorized to assess the adequacy of management, personnel and organization in the intelligence agencies. The heads of departments and agencies of the Federal Government, to the extent permitted by law, shall provide the PFIAB with access to all information that the PFIAB deems necessary to carry out its responsibilities.

Sec. 1.3. The PFIAB shall report directly to the President and advise him concerning the objectives, conduct, management and coordination of the various activities of the agencies of the Intelligence Community. The PFIAB shall report periodically, but at least semiannually, concerning its findings and appraisals and shall make appropriate recommendations for the improvement and enhancement of the intelligence efforts of the United States.

Sec. 1.4. The PFIAB shall consider and recommend appropriate action with respect to matters, identified to the PFIAB by the Director of Central Intelligence, the Central Intelligence Agency, or other Government agencies engaged in intelligence or related activities, in which the advice of the PFIAB will further the effectiveness of the national intelligence effort. With respect to matters deemed appropriate by the President, the PFIAB shall advise and make recommendations to the Director of Central Intelligence, the Central Intelligence Agency, or other Government agencies engaged in intelligence and related activities, concerning ways to achieve increased effectiveness in meeting national intelligence needs.

Part II. Oversight of Intelligence Activities

Sec. 2.1. The Intelligence Oversight Board (IOB) is hereby established as a standing committee of the PFIAB. The IOB shall consist of no more than four members appointed from among the membership of the PFIAB. The Chairman of the IOB shall be appointed by the Chairman of the PFIAB. The Chairman of the PFIAB may also serve as the Chairman of the IOB. The IOB shall utilize such full-time staff and consultants as authorized by the Chairman of the PFIAB.

Sec. 2.2. The IOB shall:

- (a) prepare for the President reports of intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive;
- (b) forward to the Attorney General reports received concerning intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive;

(c) review the internal guidelines of each agency within the Intelligence Community that concern the lawfulness of intelligence activities;

(d) review the practices and procedures of the Inspectors General and General Counsel of the Intelligence Community for discovering and reporting intelligence activities that may be unlawful or contrary to Executive order or Presidential directive; and

(e) conduct such investigation as the IOB deems necessary to carry out its functions under this order.

Sec. 2.3. The IOB shall, when required by this order, report to the President through the Chairman of the PFIAB. The IOB shall consider and take appropriate action with respect to matters identified by the Director of Central Intelligence, the Central Intelligence Agency or other agencies of the Intelligence Community. With respect to matters deemed appropriate by the President, the IOB shall advise and make appropriate recommendations to the Director of Central Intelligence, the Central Intelligence Agency and other agencies of the Intelligence Community.

Sec. 2.4. The heads of departments and agencies of the Intelligence Community, to the extent permitted by law, shall provide the IOB with all information that the IOB deems necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community, to the extent permitted by law, shall report to the IOB at least on a quarterly basis and from time to time as necessary or appropriate, concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

Part III. General Provisions

Sec. 3.1. Information made available to the PFIAB, or members of the PFIAB acting in their IOB capacity, shall be given all necessary security protection in accordance with applicable laws and regulations. Each member of the PFIAB, each member of the PFIAB's staff and each of the PFIAB's consultants shall execute an agreement never to reveal any classified information obtained by virtue of his or her services with the PFIAB except to the President or to such persons as the President may designate.

Sec. 3.2. Members of the PFIAB shall serve without compensation but may receive transportation expenses and per diem allowance as authorized by law. Staff and consultants to the PFIAB shall receive pay and allowances as authorized by the President.

Sec. 3.3. Executive Order No. 12334 of December 4, 1981, as amended, and Executive Order No. 12537 of October 28, 1985, as amended, are revoked.

William J. Clinton
THE WHITE HOUSE
September 13, 1993.

~~FOR OFFICIAL USE ONLY~~

ASSISTANT TO THE SECRETARY OF DEFENSE
(INTELLIGENCE OVERSIGHT)
OUTREACH PROGRAM (U)

~~(FOUO)~~ **Marshall Center Initiative:** In the spirit of promoting democratic principles under the rubric of Partnership for Peace, ATSD (IO) initiated a seminar at the George C. Marshall European Center for Security Studies, which presents the concept of intelligence oversight in the U.S. Defense Department, explains why we have such an oversight system, and discusses how it might be applicable to emerging central and eastern Europe in democracies. This program, which has received high marks from the Marshall Center, has been taught to more than 50 mid-level future leaders from the nations of the former Warsaw Pact. It captures the essence of what then-Secretary of Defense Cheney hoped to achieve when he approved DoD Directive 5200.34, creating the Center more than eight years ago. It was his intention to "seek out civilian and military defense and policy officials of the former Soviet republics and offer them a solid educational foundation in democratic defense management."

~~(FOUO)~~ **School of Americas Initiative (the school was recently closed and is reopening as the Western Hemisphere Institute for Security Cooperation):** Recognizing the public perception problems faced by the former School of the Americas, the ATSD (IO) offered the Secretary of the Army a program on intelligence oversight and its democratic foundation principles in the U.S. Defense Department, similar to what we developed and presented at the Marshall Center. The first presentation was delivered and warmly received by 60 Latin American and U.S. military students at the last class just before the School of the Americas was closed. We have been invited to continue the seminar program next year when the school reopens as the Western Hemisphere Institute for Security Studies. Both this and the Marshall Center program offer these future leaders from Europe and Latin America keen insights into how military and civilian leaders in the U.S. balance national security needs with constitutionally guaranteed rights of US persons.

~~(FOUO)~~ **Africa Center, Asia-Pacific Center Initiative Planning:** The ATSD (IO) has offered to these centers programs similar to those being conducted at the Marshall Center and the Western Hemisphere Institute for Security Studies. Both of these efforts are still in the pre-planning phase.

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED

CDSN = HPA388 MCI = 98322/17863 TOR = 98:441447
PTTUZYUW RUEKJCS86.9 3221625-UUUU--RHCUAJ. RHHMUNA RUCJAAA RUCJACC
RUCUSTR RUCXNLG RUDHAAA RUDHNIS RUEAADN RUEAHC RUEADWD RUEAHQA
RUEAIJU RUEAUSA RUEBMJB RUEDADI RUEKDIA RUEKCS RUENAAA RUETIAA
RUFGNOA RULSMCA RULYSCC RUMIAAA RUFEUNA RUQVIA RUWMFBA.
ZNR UUUUU

P 181700Z NOV 98

FM SECDEF WASHINGTON DC//ATSD-IO//
TO RUEKJCS/JOINT STAFF WASHINGTON DC//OJCS-LI/DJS/IG/J2/J3//
RUEADWD/SECARMY WASHINGTON DC//SAIG-IO/GC//
RUENAAA/SECNAV WASHINGTON DC//NAVJCSGEN/GC//
RUEAHQA/OSAF WASHINGTON DC//SAF-IGI/GC//
RUEADWD/CSA WASHINGTON DC//JACS/DAFI/DAJA/DAIO/DAAR//
RUENAAA/CNO WASHINGTON DC//N00/N09/N095/N1/N5/NLSC//
RUEAHQA/CSAF WASHINGTON DC//CC/CV/XO/XOI/CAG, AF-RE//
RUEACHC/CMC WASHINGTON DC//JMC/ACMC/IG/SJI/C1/C41/PP&O/MCRC//
RUFGNOA/USCINCEUR WASHINGTON GE//IG/J2/J3/JA//
RULYSCC/USACOM NORFOLK VA//IG/J2/J3/SJA//
RUCJACC/USCINCCENT MACDILL AFB FL//IG/J2/J3/JA//
RUCJAAA/USSOCOM MACDILL AFB FL//IG/J2/J3/JA, CORB//
RUMIAAA/USCINCSO MIAMI FL//IG/J2/J3/SJA//
RUFEUNA/USCINCSpace PETERSON AFB CO//IG/J2/J3/SJA//
RHCUAJ/USCINCTRAN SCOTT AFB IL//IG/J2/J3/SA//
RHHMUNA/USCINCPAC HONOLULU HI//IG/J2/J3/SA//
RUCUSTR/USCINCPAC OFFUTT AFB NE//IG/J2/J3/JA//
RUETIAA/DIRNSA FT GEORGE G MEADE MD//IG/GC/NOC//
RUEKDIA/DIA WASHINGTON DC//IG/J2/GC/DO/DH/DIC/DAJ/DIO/MC//
RUEBMJB/NRO WASHINGTON DC//IG/GC//
RUEAIJU/NIMA WASHINGTON DC//IG/GC//
RUEAADN/DTRA WASHINGTON DC//IG/GC/CI//
RUEAUSA/CNGB WASHINGTON DC//NGB-2A/NGB-ARI/NGB-IG//
RUEAUSA/NGB WASHINGTON DC//JF//
INFO RUEKJCS/SECDEF WASHINGTON DC//JC/IG/ISDI/C3I/ATSD-IO//
RUDHAAA/CDRINSCOM FT BELVOIR VA//CER/CS-IC/IC/DCSOPS/SJA//
RUCXNLG/ONI SUITLAND MD//IG/GC//
RUDHNIS/DIRNAVCRIM NVSERV WASHINGTON DC//G/C//
RUQVAIA/AIA KELLY AFB TX//CC/CV/IG/IN/SJA//
RUEDADI/AFOSI BOLLING AFB DC//CC/CV/IG/SJI//
RUWMFBA/AFIA KIRTLAND AFB NM//CC/IC-IO//
RULSMCA/MCIA QUANTICO VA
BT

UNCLAS SECTION 01 OF 02

SUBJECT: POLICY GUIDANCE FOR INTELLIGENCE SUPPORT TO FORCE
PROTECTION

REFERENCES:

A. EXECUTIVE ORDER 12333

PAGE 01

UNCLASSIFIED

181700Z NOV 98

B. DODD 5240.1
 C. DODD 5200.27
 D. DOD REG 5240.1-R
 E. MCM 75-91
 F. AR 381-10
 G. SECNAVINST 3820.3D
 H. AFI 14-104
 I. MCO 3800.2A
 J. DIRECTOR OF COUNTERINTELLIGENCE MEMO, "AUTHORITY TO COLLECT INFORMATION ON DOMESTIC TERRORIST AND OTHER GROUPS COMMITTING ILLEGAL ACTS THAT POSE A THREAT TO THE DEPARTMENT OF DEFENSE (U)," DATED 27 JAN 98.

1. THE PURPOSE OF THIS MESSAGE IS TO PROVIDE POLICY GUIDANCE TO COMMANDERS AND SUPPORTING DOD INTELLIGENCE ORGANIZATIONS REGARDING PERMISSIBLE INTELLIGENCE SUPPORT FOR FORCE PROTECTION ACTIVITIES.
2. THIS MESSAGE HAS BEEN COORDINATED WITH THE JOINT STAFF; THE DOD GENERAL COUNSEL; THE INSPECTOR GENERAL, DOD; THE UNDERSECRETARY OF DEFENSE FOR POLICY; AND THE SENIOR CIVILIAN OFFICIAL IN THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE.
3. FORCE PROTECTION IS A FUNDAMENTAL COMMAND RESPONSIBILITY FOR ALL COMMANDERS WHEREVER LOCATED. DOD INTELLIGENCE AND COUNTERINTELLIGENCE (INTEL/CI) COMPONENTS HAVE AN IMPORTANT ROLE TO PLAY IN SUPPORT OF THE COMMANDERS' FORCE PROTECTION MISSION. EXECUTIVE ORDER 12333 AND DOD 5240.1-R REGULATE THE CONDUCT OF INTEL/CI ACTIVITIES; THE ATTORNEY GENERAL HAS APPROVED THE PROCEDURES IN DOD 5240.1-R. THEIR PURPOSE IS TO ENABLE DOD INTEL/CI COMPONENTS TO CARRY OUT EFFECTIVELY THEIR AUTHORIZED FUNCTIONS WHILE ENSURING THAT THEIR ACTIVITIES THAT AFFECT UNITED STATES PERSONS ARE CARRIED OUT IN A MANNER THAT PROTECTS THE CONSTITUTIONAL RIGHTS AND PRIVACY OF SUCH PERSONS.
4. INTEL/CI COMPONENTS DO NOT HAVE A LAW ENFORCEMENT MISSION. LAW ENFORCEMENT IS THE RESPONSIBILITY OF THOSE AGENCIES SPECIFICALLY CHARTERED TO HANDLE LAW ENFORCEMENT MATTERS, E.G., PROVOST MARSHAL; CID; OSI; AND NCIS. (NOTE: AFOSI AND NCIS HAVE BOTH COUNTERINTELLIGENCE AND LAW ENFORCEMENT MISSIONS, WHICH ARE MANAGED SEPARATELY WITHIN THESE ORGANIZATIONS.) OFF THE INSTALLATION IN CONUS, LAW ENFORCEMENT IS THE RESPONSIBILITY OF LOCAL AND STATE LAW ENFORCEMENT OFFICIALS AND THE FBI AT THE FEDERAL LEVEL, NOT DOD INTEL/CI COMPONENTS.
5. WHEN FOREIGN GROUPS OR PERSONS THREATEN DOD PERSONNEL, RESOURCES, OR ACTIVITIES -- WHETHER CONUS OR OCONUS -- DOD INTEL/CI COMPONENTS MAY INTENTIONALLY TARGET, COLLECT, RETAIN, AND DISSEMINATE INFORMATION ON THEM (UNLESS THE GROUPS OR PERSONS IN QUESTION MEET THE DEFINITION OF UNITED STATES PERSONS IN EXECUTIVE ORDER 12333/DOD 5240.1-R - SEE PARA 11A BELOW). BOTH CONUS AND OCONUS, INTEL/CI COMPONENTS ARE RESTRICTED IN WHAT AND HOW THEY CAN COLLECT, RETAIN, AND DISSEMINATE INFORMATION WITH RESPECT TO UNITED STATES PERSONS, AS

UNCLASSIFIED

EXPLAINED BELOW.

6. COMMANDERS MAY NOT LEGALLY DIRECT DOD INTEL/CI COMPONENTS TO TARGET OR INTENTIONALLY COLLECT INFORMATION FOR FORCE PROTECTION PURPOSES ON U.S. PERSONS UNLESS SUCH PERSONS HAVE BEEN IDENTIFIED IN REFERENCE J, OF SUBSEQUENT VERSIONS. THE FBI PARTICIPATES IN THE IDENTIFICATION OF THESE PERSONS.

7. COMMANDERS SHOULD BE COGNIZANT, HOWEVER, OF THE FACT THAT DURING THE CONDUCT OF ROUTINE LIAISON ACTIVITIES, DOD INTEL/CI COMPONENTS OFTEN RECEIVE INFORMATION IDENTIFYING U.S. PERSONS ALLEGED TO THREATEN DOD RESOURCES, INSTALLATIONS, MATERIEL, PERSONNEL, INFORMATION, OR ACTIVITIES. DOD INTEL/CI ACTIVITIES MAY ACT AS A CONDUIT AND MUST PASS ANY THREAT INFORMATION INCIDENTALLY RECEIVED IN THIS MANNER TO THE THREATENED COMMANDER AND THE ENTITY WHICH HAS RESPONSIBILITY FOR COUNTERING THAT THREAT (E.G., MILITARY POLICE, PROVOST MARSHAL, OR SECURITY DIRECTOR). THIS TRANSMITTAL OF INFORMATION DOES NOT CONSTITUTE COLLECTION BY THE DOD INTEL/CI ORGANIZATION WITHIN THE MEANING OF DOD REGULATION 5240.1-R (REFERENCE D), AND IS THEREFORE PERMISSIBLE. HOWEVER, ANY FOLLOW-ON INTEL/CI INVESTIGATION, COLLECTION OR TARGETING OF SUCH U.S. PERSONS WOULD BE SUBJECT TO EXISTING PROCEDURES AS SET FORTH IN REFERENCES A THROUGH J.

8. LAW REFERENCE C, DOD LAW ENFORCEMENT AND SECURITY ORGANIZATIONS -- AS OPPOSED TO INTEL/CI COMPONENTS -- MAY LEGALLY ACCEPT AND RETAIN FOR UP TO 90 DAYS, UNLESS LONGER RETENTION IS REQUIRED BY LAW OR PERMISSION IS SPECIFICALLY GRANTED BY THE SECRETARY OF DEFENSE OR HIS DESIGNEE INFORMATION PERTAINING TO U.S. PERSONS WHICH THREATENS DOD RESOURCES, PERSONNEL, INSTALLATIONS, MATERIEL, INFORMATION, OR ACTIVITIES. COMMANDERS SHOULD TAKE APPROPRIATE ADVANTAGE OF LAW ENFORCEMENT LIAISON ACTIVITIES TO MONITOR CRIMINAL ACTIVITY IN THE VICINITY OF THEIR INSTALLATIONS/ACTIVITIES (ACTS OF TERROR, ASSAULT, THREATS OF HARM, OR DESTRUCTION OF GOVERNMENT PROPERTY ARE CRIMINAL ACTS).

9. TO CLARIFY THE ROLE OF DOD INTEL/CI ORGANIZATIONS IN SUPPORTING COMMANDERS' FORCE PROTECTION RESPONSIBILITIES, THE FOLLOWING GUIDANCE IS EFFECTIVE ON RECEIPT:

A. WHEN DOD INTEL/CI ORGANIZATIONS LEARN OF INFORMATION PRESENTING A REASONABLE BELIEF THAT A U.S. PERSON OTHER THAN A PERSON IDENTIFIED BY THE DOD DIRECTOR OF COUNTERINTELLIGENCE (IN REFERENCE J) POSES A THREAT TO DEPARTMENTAL RESOURCES, PERSONNEL, INSTALLATIONS, MATERIEL, INFORMATION, OR ACTIVITIES, THE ACQUIRING UNIT SHALL IMMEDIATELY ALERT THE APPROPRIATE OFFICIAL OF THE THREATENED ENTITY AND PROVIDE THE INFORMATION TO THE APPROPRIATE LAW ENFORCEMENT AUTHORITY. FOLLOWING SUCH NOTIFICATION, IF THE ACQUIRING UNIT HAS REASON TO PERMANENTLY RETAIN THAT INFORMATION UNDER THE PROVISION OF PROCEDURE 3 OF DOD REGULATION 5240.1-R, IT SHALL REQUEST, BY THE MOST EXPEDITIOUS MEANS AVAILABLE AND THROUGH ITS SERVICE INTELLIGENCE COMPONENT, THAT OSD(C3I) EVALUATE THE ACQUIRED INFORMATION FOR

***** PAGE 03

UNCLASSIFIED

181700Z NOV 98
/

.....
* UNCLASSIFIED *

RETENTION ("COLLECTABILITY DETERMINATION"). OASD(CJI) WILL
COORDINATE THE REQUEST WITH THE DOD GENERAL COUNSEL AND THE
ATSD(IO) PRIOR TO NOTIFYING THE SERVICE INTELLIGENCE COMPONENT OF
APPROVAL/DISAPPROVAL OF THE REQUEST. THE MILITARY SERVICES ARE
ENJOINED TO PROCESS COLLECTABILITY DETERMINATIONS EXPEDITIOUSLY.
B. WHILE AWAITING A COLLECTABILITY/RETAINABILITY
BT
#8619

NN

..... PAGE 04
* UNCLASSIFIED * 181700Z NOV 98
..... /

UNCLASSIFIED

CDSN = HPA395 MCN = 98321/17940 TOR = 983441450
PTTUZYUW RUEKJCS8620 3221616-UUUU- RHCUAAA RHHMUNA RUCJAAA RUCJACC
RUCUSTR RUCXNLG RUDHAAA RUDHNIS RUADN RUEATMC RUEADWD RUEAHQA
RUEAIJU RUEAUSA RUEBMJB RUADADI RUEKDIA RUEKJCS RUENAAA RUETIAA
RUFNGOA RULSMCA RULYSCC RUMIAAA RUPEUNA RUQVAIA RUWMFBA.

ZNR UUUUU

P 181700Z NOV 98

FM SECDEF WASHINGTON DC//A/SD-IO//
TO RUEKJCS/JOINT STAFF WASHINGTON DC//OJCS-LA/DJS/IG/J2/J3//
RUEADWD/SECARMY WASHINGTON DC//SAI-IO/GC//
RUENAAA/SECNAV WASHINGTON DC//NAVJCSGEN/GC//
RUEAHQA/OSAF WASHINGTON DC//SAF-IG/GC//
RUEADWD/CSA WASHINGTON DC//DACS/DAI/DAJA'DA40/DAAR//
RUENAAA/CNO WASHINGTON DC//N00/N09,N095/N2/N3/N5/NLSC//
RUEAHQA/CSAF WASHINGTON DC//CC/CV/O/XOI/TAG'AF-RE//
RUEACMC/CMC WASHINGTON DC//CMC/ACMC/IG/SJA/C/C4I/PP&O/MCRC//
RUFNGOA/USCINCEUR VAIHINGEN GE//IG/J2/J3/SJA//
RULYSCC/USACOM NORFOLK VA//IG/J2/J3/SJA//
RUCJACC/USCINCCENT MACDILL AFB FL//IG/J2/J3/SJA//
RUCJAAA/USSOCOM MACDILL AFB FL//IG/J2/J3/SJA/CORB//
RUMIAAA/USCINCSO MIAMI FL//IG/J2/J3/SJA//
RUPEUNA/USCINCSpace PETERSON AFB CA//IG/J2/J3/SJA//
RHCUAAA/USCINTRANS SCOTT AFB IL//IG/J2/J3/SJA//
RHHMUNA/USCINCPAC HONOLULU HI//IG/J2/J3/SJA//
RUCUSTR/USCINSTRAT OFFUTT AFB NE//IG/J2/J3/SJA//
RUETIAA/DIRNSA FT GEORGE G MEADE MD//IG/GC/NSOC//
RUEKDIA/DIA WASHINGTON DC//IG/J2/GC/DO/DHS/DAC/DAJ/DIO/MC//
RUEBMJB/NRO WASHINGTON DC//IG/GC//
RUEAIJU/NIMA WASHINGTON DC//IG/GC//
RUEAADN/DTRA WASHINGTON DC//IG/GC/CI//
RUEAUSA/CNGB WASHINGTON DC//NGB-ZA,NGB-ARZ/NGB-IG//
RUEAUSA/NGB WASHINGTON DC//CF//
INFO RUEKJCS/SECDEF WASHINGTON DC//GC/IG/JSD/C3I/ATSD-IO//
RUDHAAA/CDRINSCOM FT BELVOIR VA//CDR/CS-IO/IG/DCSOPS/SJA//
RUCXNLG/ONI SUITLAND MD//IG/GC//
RUDHNIS/DIRNAVCRIP INVSERV WASHINGTON DC//IG/GC//
RUQVAIA/AIA KELLY AFB TX//CC/CV/IG,IN/SJA//
RUEDADI/AFOSI BOLLING AFB DC//CC/CV/IG/SJA//
RUWMFBA/AFIA KIRTLAND AFB NM//CC/IG-IO//
RULSMCA/MCIA QUANTICO VA

BT

UNCLAS FINAL SECTION OF 02

DETERMINATION, THE ACQUIRING UNIT MAY INDEX THE INFORMATION AND
MAINTAIN IT ON FILE FOR A 90 DAY PERIOD. IF, DURING THAT
90 DAY PERIOD, THE ACQUIRING UNIT EARNS OF ADDITIONAL
INFORMATION RELATING TO THE THREAT POSED BY THE U.S. PERSON IN

PAGE 01

UNCLASSIFIED

181700Z NOV 98

QUESTION, THE UNIT SHALL IMMEDIATELY PASS THAT INFORMATION TO THE APPROPRIATE OFFICIAL OR LAW ENFORCEMENT AUTHORITY. (THIS INFORMATION MAY BE DISSEMINATED TO AFFECTED COMMANDERS AND SECURITY OFFICIALS, ONLY.)

C. IF OASD(C3I) DENIES PERMISSION TO COLLECT OR RETAIN INFORMATION ON THE U.S. PERSON, THE REQUESTING ORGANIZATION WILL REMOVE ALL INFORMATION PERTAINING TO THAT U.S. PERSON FROM ITS FILES AND DESTROY IT OR TRANSFER IT TO A DOD LAW ENFORCEMENT OR SECURITY ACTIVITY WHICH HAS AN OFFICIAL NEED FOR THE INFORMATION. OASD(C3I) WILL PROVIDE TO OATSD(IO) AND THE GENERAL COUNSEL, WITHIN FIVE WORKING DAYS, ONE COPY OF ALL PERMISSIONS TO COLLECT/RETAIN INFORMATION ON U.S. PERSONS NOT LISTED IN REFERENCE J. WITHIN 30 DAYS OF RECEIPT OF THIS MESSAGE, HEADS OF DOD INTEL/CI COMPONENTS WILL PROVIDE TO OATSD(IO) ONE COPY OF ANY INSTRUCTIONS ISSUED WHICH IMPLEMENT THIS MESSAGE.

10. REQUEST HEADS OF DOD INTEL/CI COMPONENTS ENSURE THAT ALL FIELD LOCATIONS PROVIDING INTELLIGENCE SUPPORT TO COMMANDERS RECEIVE A COPY OF THIS MESSAGE.

11. ADDRESSEES ARE INVITED TO VISIT OUR RECENTLY ACTIVATED ATSD(IO) HOMEPAGE ON THE INTERNET AT WWW.DTIC.MIL/ATSDIO.

12. DEFINITIONS:

A. FROM APPENDIX A, DOD REGULATION 5240.1-R:

(1) THE TERM "U.S. PERSONS" MEANS:

- (A) A U.S. CITIZEN;
- (B) AN ALIEN KNOWN BY THE DOD INTELLIGENCE COMPONENT CONCERNED TO BE A PERMANENT RESIDENT ALIEN (PRA);
- (C) AN UNINCORPORATED ASSOCIATION SUBSTANTIALLY COMPOSED OF U.S. CITIZENS OR PRAS;
- (D) A CORPORATION INCORPORATED IN THE U.S., EXCEPT FOR A CORPORATION DIRECTED AND CONTROLLED BY A FOREIGN GOVERNMENT OR GOVERNMENTS. A CORPORATION OR CORPORATE SUBSIDIARY INCORPORATED ABROAD, EVEN IF PARTIALLY OR WHOLLY OWNED BY A CORPORATION INCORPORATED IN THE U.S., IS NOT A U.S. PERSON.

A PERSON OR ORGANIZATION OUTSIDE THE U.S. SHALL BE PRESUMED NOT TO BE A U.S. PERSON UNLESS SPECIFIC INFORMATION TO THE CONTRARY IS OBTAINED. AN ALIEN IN THE U.S. SHALL BE PRESUMED NOT TO BE A U.S. PERSON UNLESS SPECIFIC INFORMATION TO THE CONTRARY IS OBTAINED.

A PERMANENT RESIDENT ALIEN IS A FOREIGN NATIONAL LAWFULLY ADMITTED INTO THE U.S. FOR PERMANENT RESIDENCE AND, THEREFORE, IS A U.S. PERSON.

(2). FOREIGN INTELLIGENCE IS INFORMATION RELATING TO THE CAPABILITIES, INTENTIONS, AND ACTIVITIES OF FOREIGN POWERS, ORGANIZATIONS, OR PERSONS, BUT NOT INCLUDING COUNTERINTELLIGENCE EXCEPT FOR INFORMATION ON INTERNATIONAL TERRORIST ACTIVITIES.

(3). COUNTERINTELLIGENCE IS INFORMATION GATHERED AND ACTIVITIES CONDUCTED TO PROTECT AGAINST ESPIONAGE, OTHER INTELLIGENCE

.....
* UNCLASSIFIED *

ACTIVITIES, SABOTAGE, OR ASSASSINATIONS CONDUCTED FOR OR ON BEHALF OF FOREIGN POWERS, ORGANIZATIONS, OR PERSONS. OR INTERNATIONAL TERRORIST ACTIVITIES, BUT NOT INCLUDING PERSONNEL, PHYSICAL, DOCUMENT, OR COMMUNICATIONS SECURITY PROGRAMS.

B. FROM JOINT PUB 2-01, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, DATED 23 MAR 84: FORCE PROTECTION IS DEFINED AS "SECURITY PROGRAM DESIGNED TO PROTECT SOLDIERS, CIVILIAN EMPLOYEES, FAMILY MEMBERS, FACILITIES, AND EQUIPMENT, IN ALL LOCATIONS AND SITUATIONS, ACCOMPLISHED THROUGH PLANNED AND INTEGRATED APPLICATION OF COMBATING TERRORISM, PHYSICAL SECURITY, OPERATIONS SECURITY, PERSONAL PROTECTIVE SERVICES, AND SUPPORTED BY INTELLIGENCE, COUNTERINTELLIGENCE, AND OTHER SECURITY PROGRAMS."

BT

#8620

NN

***** PAGE 03

* UNCLASSIFIED

* 181700Z NOV 98

/