8/15/79

July 12, 1979
NUMBER

Department of Defense Directive

SUBJECT Activities of DoD Intelligence Components that Affect United States Persons

References:
(a) Executive Order 12036, "United States Intelligence Activities," January 24, 1978
(b) Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511
(c) Posse Comitatus Act, 18 U.S.C.A. § 1385 (1976)
(d) 26 U.S.C.A. § 6103 (1976)
(e) Presidential Directive/NSC-9, March 30, 1977
(f) DoD Directive 1000.17, "Department of Defense Personnel Assigned to Duty Outside the Department and Supporting Non-DoD Activities," May 31, 1977
(g) DoD Directive 5030.34, "Agreement Between the United States Secret Service and the Department of Defense Concerning Protection of the President and Other Officials," July 11, 1977
(h) DoD Directive 5030.49, "Customs Inspection," September 23, 1971
(i) DoD Directive 5105.42, "Defense Investigative Service," July 19, 1978
(j) DoD Directive 5100.23, "Administrative Arrangements for the National Security Agency," May 17, 1967
(k) DoD Directive 5100.82, "Inspector General for Defense Intelligence," June 30, 1976
(l) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," December 8, 1975
(m) DoD Directive 5210.64, "Alternate Joint Communications Center Protection Program," November 6, 1978
(n) DoD/FBI, "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," April 5, 1979

A. PURPOSE

This Directive implements Executive Order 12036 and the Foreign Intelligence Surveillance Act of 1978. It provides the authority under which Department of Defense intelligence and communications security components may collect, store or disseminate information about United States persons.

Procedures previously approved by the Attorney General are hereby superceded except procedures approved pursuant to Presidential Directive/NSC-9 (ref. (e)).

B. APPLICABILITY AND SCOPE

This Directive applies to all intelligence components of the Department of Defense. This Directive applies only to the intelligence activities of Department of Defense intelligence components. It does not apply to law enforcement activities.

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 3.

D. POLICY

1. The intelligence activities of the Department of Defense that involve United States persons are implemented taking account of the paramount importance of the protection of the constitutional rights and privacy of the American people. In approving activities under these procedures, responsible officials shall ensure that information concerning United States persons is gathered by the least intrusive means possible.

2. Executive Order 12036 requires the Department of Defense to promulgate procedures for carrying out certain kinds of intelligence activities and for use of certain information-gathering techniques. Procedures that require approval by the Attorney General have been submitted and approved in accordance with the Order. These procedures are set out in enclosure 1, Procedures that require approval only by the Secretary of Defense are set out in enclosure 2. All DoD guidance with respect to Executive Order 12036 is consolidated in this Directive.

3. The procedures set out in enclosures 1 and 2 contain restrictions and prohibitions on actions by or on behalf of Department of Defense intelligence components. These

restrictions and prohibitions are to be interpreted strictly. No intelligence component may request or otherwise encourage, directly or indirectly, any person, organization, or government agency to undertake activities restricted or prohibited by these procedures.

4. Violations of Executive Order 12036 or of this Directive, whether intentional or unintentional, shall be reported promptly to an inspector general or general counsel with responsibility for the DoD intelligence component where the violation occurred or to the Inspector General for Defense Intelligence. Prompt reporting will help curb errors, correct mistaken interpretations of the Order, eliminate or prevent activities that are illegal, and provide helpful oversight within the DoD system.

5. The procedures in enclosure 1 do not authorize every DoD intelligence component to engage in every intelligence activity regulated therein.

E. RESPONSIBILITIES AND FUNCTIONS

1. The head of each DoD intelligence component shall ensure that the requirements of this Directive are followed scrupulously.

2. The Secretaries of the Military Departments shall provide for implementation of procedures that permit issuance of warrants by military judges by making the necessary arrangements for availability, scheduling, and security measures of military judges.

3. The Inspector General for Defense Intelligence shall provide a central focal point for contact with and reporting to the Intelligence Oversight Board. Reports by general counsels and inspectors general shall be forwarded to the Intelligence Oversight Board by the Inspector General for Defense Intelligence together with appropriate additional information or comments. The Inspector General for Defense Intelligence shall review the reporting system periodically in order to reduce paperwork and administrative burden.

4. The Department of Defense General Counsel shall provide a central focal point for contact with and reporting to the Attorney General. Requests for Attorney General approval shall be forwarded to the Department of Defense General Counsel for coordination prior to transmission to the Attorney General. The General Counsel is responsible for interpreting this Directive (and the procedures in Enclosures 1 and 2),

Executive Order 12036, and the Foreign Intelligence Suveillance Act. The General Counsel shall consult with the Attorney General where significant new legal issues are involved.

5. The general counsel and inspector general with responsibilities for each intelligence component shall monitor the oversight system within the component that is intended to detect and prevent violations of Executive Order 12036 and this Directive. Reports of activities that raise questions of illegality or impropriety shall be forwarded to the Inspector General for Defense Intelligence. The general counsels and inspectors general shall provide such other reports or information as the Inspector General for Defense Intelligence may require.

F. IMPLEMENTING INSTRUCTIONS

No implementing instruction with respect to this Directive, Executive Order 12036, or the Foreign Intelligence Act of 1978 may be promulgated without clearance by the Department of Defense General Counsel.

G. EFFECTIVE DATE

This Directive is effective immediately.

Secretary of Defense

Enclosures - 4
1. Procedures approved by the Attorney General and the Secretary of Defense
2. Procedures approved by the Secretary of Defense
3. Definitions
4. Classified Annex

PROCEDURE 1. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

Sec. 1. Applicability and Scope

This procedure governs the means that may be used and the kind of information about United States persons that may be collected without their consent. These limitations apply regardless of the means used to collect the information and they apply to the collection efforts of all DoD intelligence components. These limitations do not apply when the information is--

- available publicly;
- collected with the consent of the person whom the information concerns;
- about persons or organizations that do not qualify as United States persons; or
- collected for law enforcement purposes.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- agent of a foreign power
- available publicly
- clandestine intelligence activity
- commercial organization
- consent
- contact
- contractor
- corporation
- counterintelligence
- counterintelligence investigation
- DoD intelligence component
- employee
- foreign intelligence
- foreign power
- intelligence community
- intelligence method
- intelligence source

- international terrorist activities
- law enforcement
- law enforcement authorities
- lawful investigation
- narcotics production or trafficking
- personnel security
- personnel security investigation
- physical security
- physical security investigation
- reasonable belief
- United States
- United States person

Collection. Information is not "collected" by human intelligence operations until it is communicated by an employee to an entity of the intelligence community by filing of reports or other means. DoD intelligence components operate offices that conduct liaison with foreign governments on behalf of United States government agencies. When passing information between such agencies and foreign governments, these offices will be considered to have "collected" the information (for which they are a conduit) only if an office stores the information or disseminates the information within the intelligence component that operates the office.

Where consent to a particular collection activity is implied on the basis of adequate notice that a particular action (such as entering a restricted area) presumes consent to an accompanying action (such as search of briefcases), the adequacy of notice implying consent should be determined by the General Counsel of the intelligence component. Significant questions as to adequacy of notice in particular cases shall be referred to the DoD General Counsel, who will consult with the Attorney General where significant new legal issues are involved.

Cooperating sources in this context means persons or organizations that volunteer information to DoD intelligence components, or provide information at the request of such components. These include government agencies, law enforcement authorities, credit agencies, academic institutions, employees, foreign governments, and others who provide information on a voluntary basis. Inquiries made of cooperating sources must include identification of the Department of Defense or a component thereof.

Sec. 3. Policy

The Department of Defense collects information about United States persons for foreign intelligence and counterintelligence purposes only when necessary to the conduct of intelligence functions assigned to the Department. The collection of information is limited carefully to avoid, where feasible, information not necessary to the conduct of these functions. Collection is accomplished by the least intrusive means that will provide foreign intelligence or counterintelligence of the quality, scope and timeliness required.

Sec. 4. Procedures

A. General criteria for collection. Information about a United States person may be collected only:

1. From sources that provide information that is available publicly;

2. From cooperating sources;

3. From collection activities undertaken with the consent of a United States person authorized to grant such consent; or

4. From intelligence collection techniques conducted in compliance with the procedures set out in this enclosure or enclosure 2.

B. Foreign intelligence. Information may be collected about a United States person under the restrictions set forth in this section if the information qualifies as foreign intelligence or, as regards potential sources or potential contacts, supports collection of foreign intelligence. The means of collection must meet the criteria set out in Section 4(A). Intentional collection must be limited to collection of information about United States persons in one of the following categories:

1. The information is about--

   (a) a person who is reasonably believed to be an officer or employee of a foreign power, or

   (b) an entity that is owned or controlled, directly or indirectly, by a foreign power; or

   (c) a person who is reasonably believed to be acting on behalf of a foreign power.

2. The information is about a person who is reasonably believed to be a potential source of foreign intelligence or a potential contact who will lead to a potential source of foreign intelligence. The information that may be collected about a United States person who is reasonably believed to be a potential source or contact is limited to that necessary for the purpose of determining the suitability or credibility of such persons.

A potential source is a person who is situated by knowledge, training, position or responsibility so as to have access to or be able to obtain or develop foreign intelligence. A potential contact is a person who is situated by acquaintance, friendship, affiliation, position or other factor so as to be able to have contact with a potential source.

3. The information is about a person who is reasonably believed to be engaged in international terrorist activities.

A person is "engaged in" an activity if that person has taken some action in furtherance of the activity or that person is in contact with a person or organization that has taken such action under circumstances that support a reasonable belief that action by the person in furtherance of the activity will follow.

4. The information is about a corporation or commercial organization.

An organization that uses the words "Inc.", "Corp.", "Co.", "Ltd.", or other common commercial designations in its name may be treated as a corporation or commercial organization for this purpose.

5. The information is about a United States person who is reasonably believed to be a captured prisoner of war or who is missing in action.

C. Counterintelligence. Information may be collected about a United States person for counterintelligence purposes under the restrictions set forth in this section. The means of collection must meet the criteria set out in Section 4(A). Intentional collection must be limited to collection of information about United States persons in one of the following categories:

1. The information is about a United States person whom facts and circumstances indicate is or may be engaged in clandestine intelligence activities on behalf of a foreign power or international terrorism and that person is--

   (a) a person who is reasonably believed to be an officer or employee of a foreign power;

   (b) an entity that is owned or controlled, directly or indirectly, by a foreign power;

   (c) a person who is in contact with a foreign power or an agent of a foreign power; or

   (d) a commercial organization.

2. The information is needed to identify a person who is in contact with someone who is the subject of a lawful counterintelligence investigation. The information that may be collected about the United States person who is in contact with the subject of the counterintelligence investigation is limited to information necessary to identify that person, including name, address, employment, and security clearance.

   A person is the "subject of" a counterintelligence investigation when the investigation has focussed on that person's activities.

3. The information is about a person who is reasonably believed to be a potential source of counterintelligence or a potential contact who will lead to a potential source of counterintelligence. Information collected about a United States person who is reasonably believed to be a potential source or a potential contact shall be limited to that necessary for the purpose of determining the suitability or credibility of such persons.

A potential source is a person who is situated by knowledge, training, experience, position, or responsibility so as to have access to or be able to obtain or develop counterintelligence. A potential contact is a person who is situated by acquaintance, friendship, affiliation, position or other factor to be able to have contact with a potential source.

D. Intelligence sources and methods. Information may be collected about a United States person if it is necessary to protect an intelligence source or method from unauthorized disclosure. The means of collection must meet the criteria in Section 4(A). Intentional collection must be limited to collection of information about United States persons in one of the following categories:

1. Information about persons who are--

(a) present employees of a DoD intelligence component;

(b) former employees of a DoD intelligence component;

The term "former employee" includes employees of predecessor components of DoD intelligence components.

(c) applicants for employment with a DoD intelligence component;

The term "applicant" in this context means a person who has made a request that he or she be considered for employment. This includes applicants for transfer to a DoD intelligence component.

(d) present contractors of a DoD intelligence component;

(e) present or former employees of a present contractor of a DoD intelligence component;

(f) former contractors of a DoD intelligence component; or

(g) present or former employees of a former contractor of a DoD intelligence component.

2. Information that is needed to identify a person in contact with a person covered by subsection 1 above.

The information that may be collected about the United States person under this subsection is limited to information necessary to identify that person, including name, address, employment, and security clearance.

E. Physical security. Information may be collected about a United States person for the purpose of protecting the physical security of DoD components and contractors that serve such components if such protection is within the assigned mission of the collecting agency. This information must be collected in the course of a lawful physical security investigation. The means of collection must meet the criteria set out in section 4(A). Intentional collection must be limited as follows:

1. Information may be collected about persons who are--

(a) discovered on a defense or intelligence installation without authorization;

(b) discovered in a portion of a defense or intelligence installation under circumstances such that there is a reasonable belief that such person is violating or is about to violate laws or regulations relating to the protection of classified information;

(c) reasonably believed to be engaging in activities that are directed at or will

result in unauthorized entry onto, or damage to an installation; or

(d) reasonably believed to jeopardize an intelligence operation because of physical proximity to the operation.

Information collection within the United States under subsections (c) and (d) with respect to a person who is not on a DoD installation should be collected only in conformity with the agreement between the Department of Defense and the Federal Bureau of Investigation dated April 5, 1979, ref. (n).

2. Information may be collected that describes the person's--

(a) identification,

(b) location, or

(c) activities, intentions and capabilities that pose a clear threat to the physical security of the intelligence component.

F. Personnel security. Information may be collected about a United States person for personal security purposes. The information must be collected in the course of a lawful personnel security investigation.

1. Within the United States, the Defense Investigative Service conducts personnel security investigations for DoD intelligence components in accordance with DoD Directive 5105.42, ref. (i), and the National Security Agency conducts certain personnel security investigations under DoD Directive 5100.23, ref. (j). DoD intelligence components are authorized to collect personnel security information from cooperating sources as needed for determination as to whether a personnel security investigation is warranted.

2. Outside the United States, information may be collected by a DoD intelligence component only with respect to applicants for employment, present employees, present

contractors, and present applicants for employment with or employees of contractors of that component or persons granted access to classified information collected or produced by that component.

3. Outside the United States, information may be collected by DoD intelligence components for the Defense Investigative Service, other DoD components that are authorized to conduct personnel security investigations, the Department of State, and the Federal Bureau of Investigation.

4. As a protective service, information may be collected about a United States person who is reasonably believed to be endangering the safety of a Department of Defense official or foreign official if the DoD intelligence component has been assigned responsibility by the Secretary of Defense for protection of that person.

G. Narcotics. Information may be collected about a United States person who is reasonably believed to be engaged in narcotics production or trafficking. "Narcotics production or trafficking" is a defined term and should be construed strictly. A person is "engaged in" an activity if that person has taken some action in furtherance of the activity or that person is in contact with a person or organization that has taken such action under circumstances that support a reasonable belief that action in furtherance of the activity will follow. Information collected should be limited to the person's identification; location; and activities, intentions, capabilities and associates with respect to narcotics production or trafficking.

H. Secret Service. Information may be collected about a United States person who is reasonably believed to be endangering the safety of a person protected by the United States Secret Service. Persons protected by the Secret Service include the President and his immediate family, the President-elect, former Presidents, the Vice President, the Vice President-elect, and visiting heads of state. The collection of such information should be in compliance with the Agreement between the Department of Defense and the Secret Service, as prescribed in DoD Directive 5030.34, ref. (g).

I. Department of State. Information may be collected about a United States person for the Department of State. Collection efforts must be reasonably designed to limit collection of information about a United States person to one of the following categories:

1. Information about a person who is reasonably believed to be endangering the safety of a person protected by the Department of State. Persons protected by the Department of State include heads of foreign states, official representatives of foreign governments, distinguished foreign visitors, the Secretary and Deputy Secretary of State and official representatives of the United States and their immediate families.

2. Information about a person who is abroad if the collection is in response to a request from the Department of State for support of its consular responsibilities relating to the welfare of such persons. A consular officer must submit a written request to the DoD intelligence component. The request must state that the person is

abroad and describe the information required in support of the Department of State's consular responsibilities. Information collected by DoD intelligence components should be limited to that described in the request.

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

Date of Attorney General approval: 8/15/79 GBB

Date of Secretary of Defense approval: _____

PROCEDURE 2. STORAGE OF INFORMATION ABOUT UNITED STATES PERSONS

Sec. 1. Applicability and Scope

This procedure governs the kind of information about United States persons that may knowingly be stored by a DoD intelligence component without the consent of the person that the information concerns. These limitations apply regardless of the means used to store the information and they apply to the information storage and retrieval systems of all DoD intelligence components. These limitations do not apply when the information to be stored is:

- collected with the consent of the person whom the information concerns;
- available publicly
- stored solely for administrative purposes not related to intelligence or security;
- required by law to be maintained;
- about persons or organizations that are not United States persons;
- stored for law enforcement purposes; or
- not immediately identified with a United States person because the identity of the United States person is deleted and a generic term or symbol is substituted so that information cannot be connected with an identifiable United States person. When the name of a United States person is included in a brand name, the name of a military or political doctrine or other descriptive figures of speech that do not disclose information about the United States person, the information may be treated in the same manner as if a generic term or symbol were used.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- administrative purposes
- available publicly
- consent
- counterintelligence
- DoD intelligence components
- foreign intelligence
- intelligence
- law enforcement
- physical security
- United States person

Sec. 3. Policy

The Department of Defense stores information about United States persons for foreign intelligence and counterintelligence purposes only when necessary to the conduct of authorized intelligence functions of Department of Defense components or other government agencies. Storage of information for law enforcement purposes is limited to short-term storage incident to delivery to law enforcement agencies.

Sec. 4. Procedure

A. Storage of Information Collected Under Procedure 1. Information about United States persons may be stored if it was collected pursuant to Procedure 1.

B. Storage of Information Acquired Incidentally. Information about United States persons may be stored if:

1. Its collection is incidental to authorized collection and such information could have been collected intentionally under this directive; or

2. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with Procedures 4, 5, or 6.

3. Such infromation is stored for cryptoanalytic and traffic analysis purposes.

Unless not practicable, information about United States persons acquired as a part of or incidental to collection activities authorized under this directive, shall be processed prior to storage in the following manner:

If the identification of the United States person(s) involved is necessary to the understanding of such information, it may be retained without alteration.

If the identification of the United States person(s) is not necessary to the understanding of the information contained therein, the information which identifies the United States person(s) involved shall be deleted and replaced with a symbol or generic term which conveys the desired meaning, prior to storage.

C. Storage of Information Relating to Functions of Other DoD Component or Executive 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 stored only as necessary to transmit or deliver such information to the appropriate recipients.

D. Temporary Storage. Information about United States persons may be stored temporarily, up to 90 days, solely for the purpose of determining whether that information my be stored under these procedures.

E. Storage of Other Information. Information about

United States persons other than that covered by Sections 4(A) or (B) shall be stored only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

F. Controls on Access to Stored Information. Storage systems shall be reasonably designed to limit access to information about United States persons to those with a need to know.

G. Duration of Retention. Information about United States persons retained in the files of DoD intelligence components shall be reviewed periodically if practicable to ensure that its continued retention serves the purpose for which it was collected and stored.

H. Information Acquired Prior to Effective Date. Information acquired prior to the effective date of this procedure may be stored by DoD intelligence components without being screened for compliance with this procedure or Procedure 1, if such storage was in compliance with E.O. 11905, E.O. 12036 or other applicable law. Information acquired prior to the effecti date of this procedure may be reviewed under Subsection G above if such a review is determined by the head of the component to be practicable and an economic use of resources.

Date of Attorney General approval: GHB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 3. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

Sec. 1. Applicablility and Scope

This procedure governs the kind of information about United States persons that may be disseminated, without consent, outside the DoD intelligence component that collected and processed the information. These limitations apply regardless of the means used to disseminate the information and to dissemination by all DoD intelligence components. These limitations do not apply when information is:

- disseminated with the consent of the person the information concerns;
- available publicly;
- about persons or organizations that do not qualify as United States persons;
- not immediately identified with a United States person because the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot be connected with an identifiable United States person. When the name of the United States person is included in a brand name, the name of a military or political doctrine or other descriptive figures of speech that do not disclose information about the United States person, the information may be treated in the same manner as if a generic term or symbol were used.
- disseminated solely for administrative purposes not related to intelligence or security;
- disseminated in accordance with law; or
- disseminated for law enforcement purposes.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- administrative purposes
- available publicly
- communications security
- consent
- contractor
- counterintelligence
- DoD intelligence components
- electronic surveillance
- employee
- foreign intelligence
- intelligence
- intelligence method
- intelligence source
- international terrorist activities
- law enforcement
- law enforcement agencies
- narcotics production and trafficking
- personnel security
- personnel security investigation
- physical security
- reasonable belief
- United States
- United States persons.

Sec. 3. Policy

The Department of Defense disseminates information about United States persons that was collected and stored by intelligence components pursuant to Procedures 1 and 2 only to DoD components and contractors, to federal, state and local government entities authorized to receive such information for the performance of lawful government function, and to foreign governments under approved arrangements or agreements.

Sec. 4. Procedure

A. General criteria for dissemination. Information about United States persons that identifies those persons may

be disseminated only if it is

- information that was collected under Procedure 1,
- foreign intelligence or counterintelligence gathered abroad,
- Foreign intelligence or counterintelligence that was collected from electronic surveillance conducted in compliance with Procedures 4, 5, or 6; or
- Foreign intelligence or counterintelligence that was collected from cooperating sources in the United States;

and it has been determined that each entity that is a recipient has a requirement in the performance of its official duties for the identity of the United States person, and the identity of the United States person is required for the understanding or utilization of the information.

B. Dissemination within the Department of Defense. Information about United States persons that identifies those persons may be disseminated to other components within the Department of Defense or to contractors only if it meets the criteria under Section 4(A) and, at the time the information is disseminated, it also meets one of the following criteria:

1. The information constitutes foreign intelligence or counterintelligence;

2. The information is necessary to provide for the physical security of the installation of any DoD component or the contractor to whom it is disseminated;

3. The information is necessary to provide for personnel security of the Department of Defense or the contractor to whom it is disseminated;

4. The information relates to a violation of the Uniform Code of Military Justice, 10 U.S.C. §§ 801-940 (1976), or to a violation of foreign, federal, state or local law by a DoD employee or to an activity that may occur in the future and if it occurs is likely to involve such a violation;

5. The information is necessary to provide for communications security of the United States Government;

6. The information is necessary for the protection of intelligence sources and methods;

7. The information is enciphered or reasonably believed to contain secret meaning and the actual meaning has not been ascertained; or

8. The information has been collected pursuant to a judicial warrant and the dissemination is consistent with the warrant.

Where practicable, information about United States persons that identifies those persons and is disseminated to other components within the Department of Defense should be transmitted in a manner that alerts the recipient that information about United States persons is contained therein and has been processed in accordance with these procedures.

C. Dissemination to Agencies within the Intelligence Community. Information about United States persons that identifies those persons may be disseminated to other agencies within the Intelligence Community not otherwise expressly provided for by these procedures only if it meets the criteria under Section 4(A) and, at the time the information is disseminated, it also meets one of the following criteria:

1. The information constitutes foreign intelligence or counterintelligence;

2. The information is necessary to provide for the physical security of the Department of Defense, its contractors or the agency to which it is disseminated;

3. The information is necessary to provide for the personnel security of the agency to which it is disseminated;

4. The information is necessary to provide for the communications security of the United States Government;

5. The information is necessary for the protection of intelligence sources and methods;

6. The information is necessary for the evaluation of a potential source of assistance in an foreign intelligence or counterintelligence activity

7. The information has been collected pursuant to a judicial warrant and the dissemination is consistent with the warrant; or

8. The information is necessary to provide for the physical security (including safety) of the personnel of the agency to which it is disseminated.

D. Dissemination to other federal departments and agencies. Information about United States persons that identifies those persons may be disseminated to federal government departments or agencies outside the intelligence community not otherwise expressly provided for by these prodecures, including the Executive Office of the President, only if the information meets the criteria under Section 4(A) and, at the time the information is disseminated, it also meets on of the following criteria:

1. The information constitutes foreign intelligence or counterintelligence;

2. The information is necessary to provide for the communications security of the United States Government;

3. The information was collected outside the United States for personnel security purposes in response to a request from another federal government department or agency and is desseminated to the requesting agency;

4. The information has been collected pursuant to a judicial warrant and the dissemination is consistent with the warrant;

5. The information is necessary to provide for the physical security or the personnel security (including safety) of the agency to which it is disseminated; or

6. The information is disseminated to the Attorney General as evidence of a crime under guidelines adc by the Attorney General. Dissemination under this subsection shall be through the DoD General Counsel.

E. Dissemination to FBI. Information about United States persons that identifies those persons may be disseminated to the Federal Bureau of Investigation only if it meets the criteria under Section 4(A) and, at the time the information is disseminated, it meets one of the following criteria:

1. The information constitutes foreign intelligence or counterintelligence;

2 The information relates to a violation of federal, state or local law or to an activity that may occur in the future and if it occurs is likely to involve a violation of federal, state or local law;

3. The information relates to narcotics production or trafficking activity that violates federal, state or local law or would be such a violation if the activity occurred in the United States;

4. The information relates to international terrorist activities that violate federal, state or local law or would be a violation if the activities occurred in the United States;

5. The information relates to the physical safety of a person protected by the United States Secret Service;

6. The information relates to the physical safety of a person protected by the Department of State;

7. The information relates to the physical security of the Department of Defense or it contractors;

8. The information is provided for a personnel security investigation by the FBI;

9. The information is necessary to provide for the communications security of the United States Government; or

10. The information is necessary for the protection of intelligence sources and methods.

F. Dissemination to other law enforcement authorities.

Information about United States persons that identifies those persons may be disseminated to federal, state or local law enforcement authorities only if it meets the criteria under Section 4(A) and one of the following criteria:

1. The information relates to a violation of federal, state or local law or to an activity that may occur in the future and if it occurs is likely to involve a violation of federal, state or local law;

2. The information relates to narcotics production or trafficking activity that is a violation of federal, state or local law or would be such a violation if the activity occurred in the United States; or

3. The information relates to international terrorist activities that violate federal, state or local law or would be a violation if the activities occurred in the United States.

G. Dissemination to Secret Service. Information about United States persons that identifies those persons may be disseminated to the Secret Service only if it meets the criteria under Section 4(A) and meets one of the following criteria:

1. The information relates to the physical safety of a person protected by the Secret Service including persons in facilities protected by the Secret Service; or

2. The information relates to international terrorist activities.

H. Dissemination to Department of State. Information about United States persons that identifies those persons may be disseminated to the Department of State only if it meets the criteria under Section 4(A) and is:

1. Information disseminated under Section 4(D);

2. Information that relates to international terrorist activities that violate federal, state or local law or would be a violation if the activities occurred in the United States;

3. Information that relates to the physical safety of a person protected by the Department of State; or

4. Information disseminated in response to a request for support of Department of State consular activities for the welfare of the person whom the information concer

I. Dissemination to DEA. Information may be disseminated to the Drug Enforcement Administration only if it meets the criteria under Section 4(A) and is information related to narcotics production or trafficking activity that is a violation of federal, state or local law or would be such a violation if the activity occurred in the United States.

J. Dissemination to Foreign Governments. Information about United States persons that identifies those persons may be disseminated to foreign governments only if:

1. The information is furnished in furtherance of United States interests pursuant to an agreement or understanding with such government by the United States; and

2. The information disseminated falls within one of the following categories--

   a. The information relates to a violation of foreign law or to an activity that may occur in the future and if it occurs is likely to involve a violation of foreign law;

   b. The information relates to narcotics production or trafficking activities that would violate U.S. law if the activity occurred in the United States, or that violate foreign law;

   c. The information relates to international terrorist activities that would violate U.S. law if the activities occurred in the United States, or that violate foreign law;

d. The information relates to the safety of any person;

e. The information constitutes foreign intelligence or counterintelligence; or

f. The information is enciphered or reasonably believed to contain secret meaning and the actual meaning cannot be or has not been ascertained.

K. Other Dissemination. Dissemination other than as provided in subsections 4(B) through (J) above must be approved by the 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.

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 4. GENERAL REQUIREMENTS FOR ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES

Sec. 1. Applicability and Scope

This procedure implements the Foreign Intelligence Surveillance Act of 1978, ref. (b), and applies to electronic surveillance conducted by DoD intelligence components within the United States.

Sec. 2. General Rules

A. Electronic surveillance pursuant to judicial warran

A DoD intelligence component may conduct electronic surveill within the United States pursuant to a judicial warrant iss by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978. Applications for judicial warrants will be made through the Attorney Genera only after prior clearance by the DoD General Counsel.

B. Authority to request electronic surveillance. A to approve submission of applications for electronic surv under the Foreign Intelligence Surveillance Act of 1978 limited to the Secretary of Defense, the Deputy Secretar Defense, the Secretary or Acting Secretary of a Militar Department, and the Director of the National Security A Authority to make applications shall be vested in such of DoD intelligence components as are designated by on approval authorities above.

C. Electronic surveillance in emergency situations.

A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General even though a warrant would otherwise be required. An emergency situation exists when:

1. The time required to secure the prior approval 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;

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

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

The head of any DoD intelligence component may contact the Attorney General directly in an emergency. If possible, such requests should be made through the DoD General Counsel. If a warrant is denied in a subsequent proceeding, the information collected under the emergency authorization must be destroyed unless it indicates a threat of death or serious bodily harm to any person, and the Attorney General approves retention of the information.

Date of Attorney General approval: GRB 8/15/79

Date of Secretary of Defense approval: _____

ADDENDUM TO PROCEDURE 4: IMPLEMENTATION
OF GENERAL REQUIREMENTS

Sec. 1. Applicability and Scope

Procedure 4 applies only to electronic surveillance conducted by DoD intelligence components within the United States. This procedure does not apply to:

- activities conducted with the consent of one or more of the parties surveilled; the definition of electronic surveillance includes only nonconsensual surveillance;

- electronic surveillance for law enforcement puroses; the Act provides only for collecting foreign intelligence or counterintelligence;

- electronic surveillance under Section 102(a) of the Act; those surveillances do not involve United States persons and are conducted under Attorney General certification;

- the use of electronic equipment for testing; such use is governed by Procedure 8 established under section 2-202 of Executive Order 12036, Ref. (a) and subsection 105(f)(1) of the Act;

- the use of electronic communications and surveillance equipment for training; such use is governed by Procedure 9 established under Section 2-202 of Executive Order 12036, ref. (a) and subsection 105(f)(3) of the Act;

- measures conducted within the United States for purposes of determining whether electroni surveillance equipment is being used unlawful these measures are governed by Procedure 7 established under Section 2-202 of the Execut Order and subsection 103(f)(2) of the Act; o:

- the use within the United States of televisi cameras or other electronic means of contin monitoring not directed at the acquisition wire, radio, or oral communications; use of means for the purposes of physical surveill is governed by Procedure 10 established und Section 2-203 of the Executive Order and Sc 102(b) of the Act.

Sec. 2. Definitions

The following definitions, set out in enclosure 3, are applicable to this procedure:

- agent of a foreign power
- clandestine intelligence agency
- consent
- counterintelligence
- DoD intelligence components
- electronic communications equipment
- intelligence
- international terrorist activities
- law enforcement
- physical security
- reasonable belief
- United States
- wire communication

NOTE: THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 USES DEFINITIONS THAT IN SOME INSTANCES ARE DIFFERENT FROM THOSE PRESENTED IN ENCLOSURE 3. THIS ACT GOVERNS ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES, SO FOR PURPOSES OF THIS PROCEDURE ONLY THE FOLLOWING DEFINITIONS OF "ELECTRONIC SURVEILLANCE," "FOREIGN INTELLIGENCE INFORMATION," "FOREIGN POWER," AND UNITED STATES PERSON" APPLY:

Electronic surveillance, in this context, means:

1. the acquisition by an electronic, mechanical or other surveillance device of the contents of any wire communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentional targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

2. the acquisition by an electronic, mechanical or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

3. the intentional acquisition by an electronic, mechanical or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

4. the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

Foreign Intelligence information, in this context, means:

1. information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

   (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

   (b) sabotage or international terrorism by a foreign power or an agency of a foreign power; or

   (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power, or

2. information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

   (a) the national defense or the security of the United States; or

   (b) the conduct of the foreign affairs of the United States.

Foreign power, in this context, means:

1. a foreign government, or any component thereof, whether or not recognized by the United States;

2. a faction of a foreign nation or nation, not substantially composed of United States persons;

3. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

4. a group engaged in international terrorism or activities in preparation therefor;

5. a foreign-based political organization, not substantially composed of United States persons; or

6. an entity that is directed and controlled by a foreign government or governments.

United States person, in this context, means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(2) of the Immigration and Nationality Act), an unincorporated association, a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power.

Electronic surveillance is conducted "within the United States" in this context when it is designed to intercept wire or radio communication sent by or intended to be received by a known United States person within the United States by intentionally targeting that United States person; is designe to intercept in the United States a wire communication sent t or from a person in the United States; is designed to interce a radio communication when the sender and all recipients are located within the United States under circumstances where the communicants have a reasonable expectation of privacy; or involves the installation of an electronic, mechanical, or

other surveillance device to acquire information from other than a wire or radio communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Electronic surveillance that does not fall within the above definition and that results in the incidental acquisition of communications sent from or intended for receipt within the United States does not thereby become electronic surveillance within the United States.

Sec. 3. Policy

Electronic surveillance by DoD intelligence components within the United States is conducted only pursuant to the Foreign Intelligence Surveillance Act of 1978, ref. (b).

Sec. 4. Procedures

A. Electronic surveillance pursuant to judicial warrant. Requests for judicial warrants shall include--

1. the identity, if known, or a description of the target of the electronic surveillance;

2. a statement of the facts and circumstances sufficient to support a reasonable belief that

   (a) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

   (b) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

3. a statement of the proposed minimization procedures (in most cases this will be a standard set of procedures approved by the Attorney General attached to these procedures as Annex B; these procedures can be modified where necessary to fit particular circumstances);

4. a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

5. a statement of the means by which the surveillance will be effected;

6. a statement whether physical entry is required to effect the surveillance;

7. a statement of the facts concerning all previous applications that have been made to any judge involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

8. a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained there after; and

9. whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

Each request for a warrant must include a draft of a proposed certification from the Assistant to the President for Nationa Security Affairs, the Secretary of Defense or the Deputy Secretary of Defense. The certification is required by statute to include a finding by the certifying official that-

(a) the information is foreign intelligence information;

(b) the purpose of the surveillance is to obtain foreign intelligence information;

(c) such information cannot reasonably be obtained by normal investigative techniques;

(d) the type of foreign intelligence information being sought falls into one of the statutory categories. The statutory categories are:

first, information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorist activities by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

second, information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

The certification must include a statement of the basis for the findings under subsections (c) and (d) above.

B. Authority to request electronic surveillance. In most cases, the judge will require that the DoD official who is the applicant for a warrant be present in the courtroom when the judge considers the application. Designation of officials for this purpose should be flexible.

C. Electronic surveillance in emergency situations. The Foreign Intelligence Surveillance Act of 1978 permits the Attorney General to grant emergency authorization only in limited circumstances when the factual basis exists for issuance of a warrant under Section 4(A) of Procedure 4 and surveillance for longer than 24 hours requires a warrant issued under Section 4(A). Requests for warrants subsequent to an emergency approval by the Attorney General shall be processed under Section 4(A).

Date of Secretary of Defense approval: _____

PROCEDURE 5. GENERAL REQUIREMENTS FOR ELECTRONIC SURVEILLANCE OF TARGETS OUTSIDE THE UNITED STATES

Sec. 1. Applicability and Scope

This procedure implements Section 2-202 of Executive Order 12036, ref. (a), and applies to electronic surveillance directed against the communications of a United States person who is outside the United States. This procedure does not apply to:

- activities conducted with the consent of one or more of the parties surveilled; the definition of electronic surveillance includes only nonconsensual surveillances;
- electronic surveillance for law enforcement purposes;
- electronic surveillance directed against a person who does not qualify as a United States person;
- the use of electronic surveillance equipment for training or testing; those uses are governed by Procedures 8 and 9,
- measures conducted outside the United States for purposes of determining whether electronic surveillance equipment is being used unlawfully and is being directed against United States Government facilities; those measures are governed by Procedure 7; and
- the use outside the United States of television cameras or other electronic means of continuous monitoring; that use is governed by Procedure 10.

Sec. 2. Definitions

The following definitions, set out in enclosure 3, are applicable to this procedure:

- clandestine intelligence activity
- consent
- counterintelligence
- DoD intelligence components

- electronic surveillance
- electronic surveillance equipment
- employee
- foreign intelligence
- foreign power
- international terrorist activities
- law enforcement
- physical security
- reasonable belief
- sabotage
- United States
- United States person
- wire communication

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.

The regulation of electronic surveillance under this procedure is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Procedure 4 so that the intentional interception of all wire or radio communications of United States persons is covered by one procedure or the other. The place where the electronic surveillance is conducted is not the deciding factor. Electronic surveillance of communications that originate and terminate outside the United States can be conducted from within the United States and still fall under this procedure rather than Procedure 4.

Sec. 3. Policy

Electronic surveillance by DoD intelligence components directed against the communications of a United States person who is outside the United States is conducted only pursuant to the approval of the Attorney General or in emergency circumstances the approval of a senior official of the Department of Defense.

Sec. 4. Procedure

A. Electronic surveillance pursuant to Attorney General approval. A DoD intelligence component may conduct electronic surveillance directed at a United States person if the surveillance is approved by the Attorney General. Requests for approval will be forwarded to the Attorney General through the DoD General Counsel or the NSA General Counsel. 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 --

(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 activites, or who conspires with, or knowingly aids and abets such 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.

(b) The electronic surveillance is likely to result in the collection of 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 the period of time, not to exceed 90 days, for which the electronic surveillance is required; and

7. A description of the expected dissemination of the product of the monitoring including a description of the means by which communications that are not sent or received by persons targeted will be protected from storage or dissemination.

B. Electronic surveillance in emergency situations. A DoD intelligence component may conduct electronic surveillance outside the United States directed at a United States person in emergency situations under the following limitations:

1. Senior officials of the Department of Defense designated in subsection 4 (D)(2) below may authorize electronic surveillance outside the United States directed at a United States person in emergency situations when securing a military warrant or 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 when a person's life is in danger the senior official authorizing such emergency surveillance shall make a finding that the requirements of § 4(A)(1) are met and shall notify the DoD General Counsel promptly.

3. The Attorney General shall be notified by the DoD General Counsel as soon as possible of the nature of the electronic surveillance, the circumstances surrounding its authorization, and the results thereof.

4. Electronic surveillance authorized by a senior official 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.

C. Officials authorized to request foreign electronic surveillance.

1. The following officials may authorize or request approval of foreign electronic surveillance under subsections 4(A) above --

   (a) the Secretary and Deputy Secretary of Defense;

(b) the Secretaries and Acting Secretaries of the Military Departments; or

(c) the Director of the National Security Agency.

2. Authorization for electronic surveillance under subsection 4(B) may be granted by --

(a) any civilian Presidential appointee,

(b) any general or flag officer, or

(c) any head of a DoD intelligence component.

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 7: COMMUNICATIONS SECURITY ACTIVITIES

Sec. 1: Applicability and Scope

This procedure implements Section 2-202 of Executive Order 12036, ref. (a), which refers to electronic surveillance equipment, and Section 105(f)(2) of the Foreign Intelligence Surveillance Act of 1978, ref. (b), which refers to electronic surveillance equipment. It applies to technical countermeasures and to vulnerability surveys. Nothing in this Procedure supercedes any provision of Procedure 4 or 5.

Sec. 2. Definitions

The following definitions, set out in enclosure 3, are applicable to this procedure:

- communications security
- contractor
- DoD intelligence components
- electronic surveillance
- electronic communications equipment
- foreign power
- United States
- United States person

The term technical countermeasures, when applied to activities within the United States, includes measures to determine the existence and capability of electronic surveillance equipment being used unlawfully. The term includes the use of electronic surveillance equipment and other electronic or mechanical devices necessary to determine whether facilities, communications equipment, or other equipment or devices owned or controlled by the United States Government or by Department of Defense contractors are susceptible to unlawful electronic surveillance; or to determine whether electronic surveillance

equipment is present and is being used unlawfully. When applied to activities outside the United States the requirement with respect to "unlawful" use and "unlawful" electronic surveillance does not apply; any use and any surveillance is included.

Communications security entity means each entity subject to the guidance of the Secretary of Defense, acting as the executive agent of the United States Government, and the Director, National Security Agency, acting for the Secretary in executing responsibilities as executive agent, that carries out any of the communications security activities of the United States Government.

Hearability survey means 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 receiption over time.

Sec. 3. Policy

DoD intelligence components use technical countermeasures and conduct vulnerability surveys, to the maximum extent that is practical, without interception of or interference with the communications of United States persons. The Director, National Security Agency, is assigned responsibility for communications security activities.

Sec. 4. Procedures

A. Criteria for countermeasures. A DoD intelligence component may use technical countermeasures against electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance if;

1. The use is limited in duration and scope to that necessary to determine the existence and capability of such equipment;

2. The use is solely for the purpose of determining the existence and capability of such equipment;

3. The use is at the request or with the consent of an authorized official in charge of a facility, organization or system where the countermeasures are to be undertaken; and

4. 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 except that information with respect to violations of federal law may be transmitted to the Attorney General and information with respect to violations of military law may be transmitted to the Secretary of the Military Department. A record of the types of communications and information subject to acquisition by the illegal electronic surveillance equipment may be retained. Such information may be used only to protect against unlawful electronic surveillance or to enforce criminal laws if such use outweighs the possible harm to national security.

B. Criteria for vulnerability surveys. Nonconsensual surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of

transmission facilities of communications common carriers, other private commercial entities, and entities of the Federal Government, subject to the following limitations:

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

2. No transmission may be acquired aurally;

3. No content of any transmission may be acquired by any means;

4. No transmissions may be recorded; and

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

C. Hearability surveys. The National Security Agency may conduct or may authorize the conduct of hearability surveys of telecommunications that are transmitted in the United States.

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

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

(a) The content of communication may not be recorded nor included in any report.

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

(c) 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 surveys has been conducted, the identity of such users may be obtained provided such identities may not be obtained from the content of the transmission themselves.

3. Dissemination. Reports may be disseminated only within the United States Government. Logs may not be disseminated unless required to verify results contained in reports.

D. Other communications security monitoring. Other communications security monitoring that is directed against the communications of United States persons may be conducted only with the consent of one of the parties to the communication.

Date of Attorney General approval: GBB 3/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 8. TESTING AND CALIBRATION OF ELECTRONIC EQUIPMENT

Sec. 1. Applicability and Scope

This procedure implements Section 2-202 of Executive Order 12036, ref. (a), which refers to electronic communications equipment; and Section 103(f)(1) of the Foreign Intelligence Surveillance Act of 1978, ref. (b), which refers to electronic equipment. It applies to the testing and calibration by Department of Defense intelligence components of electronic equipment that has the capability to intercept communications.

Sec. 2. Definitions

The following definitions, set out in enclosure 3, are applicable to this procedure:

- DoD intelligence components
- electronic surveillance
- employee
- United States
- United States person

Sec. 3. Policy

Testing and calibration of electronic equipment that can intercept communications is conducted, to the maximum extent that is practical, without interception of the communications of United States persons.

Sec. 4. Procedures

A. Criteria for testing and calibration. A DoD intelligence component may test and calibrate electronic equipment subject to the following limitations:

1. To the maximum extent that is practical, the following should be used --

   (a) laboratory generated signals,

   (b) Department of Defense official agency communications with consent from an appropriate DoD official,

   (c) official government agency communications with consent from an appropriate official of the originating agency,

   (d) individual government employee communications with consent from the employee, or

   (e) communications transmitted between terminals located outside the United States not used by any known United States person.

2. Where it is not practical to test electronic equipment solely against signals described in subsection A(1) above, testing may be conducted provided--

   (a) it is limited in scope and duration to that necessary to determine the capability of the equipment;

   (b) no particular United States person is targeted intentionally without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and

   (c) the test does not exceed 90 calendar days.

B. Time limitations. Where the test involves communications other than those identified in subsection (A)(1) above and a test period longer than 90 days is required, the DoD intelligence component shall submit a test proposal to the DoD General Counsel or the NSA General Counsel for transmission to the Attorney General for approval. The test proposal shall state the requirement for an extended test involving such communications, the

nature of the test, the organization that will conduct the test, and the proposed disposition of any signals or communications acquired during the test.

C. Storage and dissemination. The content of any communi- acquired during a test shall be:

1. Retained only for the purpose of determining the capability of the electronic equipment;

2. Disclosed only to persons conducting the test; and

3. Destroyed upon completion of the testing.

The technical parameters of a communication, such as frequency, modulation, and time of activity of acquired electronic signals may be retained and used for test reporting or collection avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance provided such dissemination and use are limited to testing or collection avoidance purposes. No content of any communication may be retained or used.

Date of Attorney General approval: EBB 8/15/75

Date of Secretary of Defense approval: _____

PROCEDURE 9. TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

Sec. 1. Applicability and Scope

This procedure implements Section 2-202 of Executive Order 12026, ref. (a), which refers to electronic communications equipment; and Section 104(f)(3) of the Foreign Intelligence Surveillance Act of 1978, ref. (b), which refers to electronic surveillance equipment. It applies to the training of the personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment. These procedures do not apply to

- interception of communications with the consent of one of the parties to the communication.
- training of intelligence personnel by non-intelligence components.

Sec. 2. Definitions

The following definitions set out in enclosure 3 are applicable to these procedures:

- consent
- DoD intelligence components
- electronic communications equipment
- electronic surveillance
- intelligence
- United States person

Sec. 3. Policy

Training of DoD personnel in the operation and use of eelctronic communications and surveillance equipment is conducted, to the maximum extent that is practical, without interception of the communications of United States persons who have not given consent.

Sec. 4. Procedures

A. Training guidance. The training of the personnel of 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 and Executive Order 12036 with respect to the unauthorized acquisition and use of the content of communications of United States persons.

B. Training limitations. The use of electronic communications and surveillance equipment for training purposes is permitted subject to the following limitations:

1. To the maximum extent that is practical, use of such equipment for training purposes shall be directed against intelligence targets otherwise authorized;

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; and

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

There are two exceptions to these limitations:

4. Public broadcasts, distress signals or official United States Government communications may be monitored provided that where government agency communications are monitored, the consent of an appropriate official is obtained; and

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

C. Storage and dissemination. Information collected during training that involves authorized intelligence targets may be stored in accordance with Procedure 2 and disseminated in accordance with Procedure 3. Information collected during training that does not involve authorized intelligence targets or that is acquired inadvertently shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This subsection does not apply to distress signals.

Date of Attorney General approval: GAB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 10: CONCEALED TELEVISION MONITORING AND OTHER CONCEALED MONITORING

Sec. 1: Applicability and Scope

This procedure implements Section 2-203 of Executive Order 12036, ref. (a), and Section 102(b) of the Foreign Intelligence Surveillance Act of 1978, ref. (b). It applies to concealed television and other monitoring for foreign intelligence and counterintelligence purposes conducted by a DoD intelligence component within the United States or directed against a United States person who is outside the United States. These procedures do not apply to:

- surveillance conducted with consent including appropriate general notices to employees;
- television and other monitoring for law enforcement purposes, or for physical security purposes;
- electronic surveillance for foreign intelligence and counterintelligence purposes; that is governed by Procedures 4 and 5;
- measures conducted to determine whether electronic surveillance equipment is being used unlawfully; those measures are governed by Procedure 7;
- physical surveillance by means other than concealed television and other concealed monitoring; that is governed by Procedure 13;
- television monitoring outside the United States directed against a person who is not a United States person; or
- overhead reconnaissance not directed at specific United States persons.

Sec. 2: Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- counterintelligence
- DoD intelligence components
- electronic surveillance
- employee
- foreign intelligence
- intelligence
- law enforcement
- physical security
- physical surveillance
- United States
- United States person

Concealed monitoring in this context means monitoring that is both surreptitious and continuous. Monitoring is surreptitious when it is targeted against a particular person or groups of persons and is conducted secretly for the purpose of keeping the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted against targeted persons without interruption for a substantial period of time. It does not include monitoring when television cameras are within sight although placed unobtrusively. It does not include monitoring by beepers when there is a notice affixed to the item to which the beeper is attached indicating the presence of the beeper. It does not include monitoring of space not targeted at specific persons.

Other concealed monitoring in this context means monitoring by movie cameras or radiating devices and receivers known as "beepers" or other means used for concealed monitoring. It does not include binoculars, search light or still photographic devices.

Monitoring is "within the United States" if the television camera, monitoring device or the target of the monitoring is located within the United States.

Monitoring is for physical security purposes if it is used to monitor open spaces, parking lots, corridors, entrances, exits, windows; or safes, vaults, restricted access areas, or other areas used primarily for the storage of classified material.

Sec. 3. Policy

The Department of Defense normally relies on the Federal Bureau of Investigation for concealed monitoring conducted in the United States except for activities on DoD property. Use of concealed television and other similar types of monitoring within the United States by DoD intelligence components is conducted only on installations, facilities, or property of the Department of Defense or its contractors. This limitiation does not apply to assistance furnished the Federal Bureau of Investigation under procedure 16 or Sec. 2-309 of Executive Order 12036.

Sec. 4. Procedures.

A. Television monitoring under no expectation of privacy. Judgments about reasonable expectations of privacy should be made on a case-by-case basis and only after consultation with the General Counsel of the intelligence component, and should take into account the great importance of preserving privacy. A reasonable expectation of privacy is measured against an objective standard of what a reasonable person would expect under the circumstances. There are reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal work

circumstances. The limitations on television monitoring where there is no reasonable expection of privacy are as follows:

1. A DoD intelligence component may conduct concealed television monitoring within the United States if the monitoring is conducted within a DoD installation or facility, if the person subject to monitoring does not have a reasonable expectation of privacy and if no physical trespass is used to effect the monitoring.

2. Television monitoring directed at a United States person may be conducted outside the United States if the person subject to the monitoring does not have a reasonable expectation of privacy and if no physical trespass is used to effect the monitoring.

3. Concealed television monitoring conducted under this subsection requires approval by the head of the intelligence component based on a determination that such monitoring is necessary to the conduct of assigned intelligence functions.

4. If physical trespass is involved to effect the monitoring, approval of the Attorney General or a warrant issued by a military judge is required.

B. Television monitoring where there is an expectation of privacy.

1. A DoD intelligence component may conduct concealed television monitoring under circumstances where the persons subjected to monitoring have a reasonable expectation of privacy if the monitoring has been approved by the DoD General Counsel or a general counsel with responsibility for an intelligence component and the necessary approvals by the Attorney General or warrants have been obtained. Warrants approving television monitoring conducted outside the United States may be issued by a military judge under the same standards as are required for electronic surveillance outside the United States (Procedure 5). Submissions to the Attorney General under this subsection shall be made by the DoD General Counsel.

2. Requests for concealed television monitoring under this subsection must be authorized by--

   (a) the Secretary of Defense, Deputy Secretary of Defense or Deputy Under Secretary of Defense (Policy);

   (b) the Secretaries and Acting Secretaries of the Military Departments;

   (c) the Director of the National Security Agency; or

   (d) the Director of the Defense Intelligence Agency.

C. Other concealed monitoring. Concealed monitoring by means other than television cameras may be conducted in accordance with Sections 4(A) or (B). Monitoring by use of

1. A DoD intelligence component may conduct concealed television monitoring under circumstances where the persons subjected to monitoring have a reasonable expectation of privacy if the monitoring has been approved by the DoD General Counsel or a general counsel with responsibility for an intelligence component and the necessary approvals by the Attorney General or warrants have been obtained. Submissions to the Attorney General under this subsection shall be made by the DoD General Counsel.

2. Requests for concealed television monitoring under this subsection must be authorized by --

   (a) the Secretary of Defense, Deputy Secretary of Defense or Deputy Under Secretary of Defense (Policy);

   (b) the Secretaries and Acting Secretaries of the Military Departments;

   (c) the Director of the National Security Agency; or

   (d) the Director of the Defense Intelligence Agency.

C. Other concealed monitoring. Concealed monitoring by means other than television cameras may be conducted in accordance with Sections 4(A) or (B). Monitoring by use of

night vision devices or telescopic vision devices may be approved under Section 4(A) if these devices are not directed against building interiors in which there is a reasonable expectation of privacy.

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

night vision devices or telescopic vision devices may be approved under Section 4(A) if these devices are not directed against building interiors in which there is a reasonable expectation of privacy.

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 11: PHYSICAL SEARCH

Sec. 1. Applicability and Scope

This procedure implements section 2-204 of Executive Order 12036, ref (a), and applies to 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. This procedure does not apply to:

- physical searches authorized pursuant to the Uniform Code of Military Justice or the Manual for Courts Martial, including command inspections or to other physical searches for law enforcement purposes;
- use of electronic or mechanical devices within the United States governed by Procedures 4, 6, 7, 8, 9 and 10;
- mail searches governed by Procedure 12; or
- searches outside the United States involving persons who are not United States persons.
- unconsented physical searches within the United States and within a Defense facility when there is an immediate threat to the safety of individuals or to prevent destruction or loss of government property where the cooperation of local law enforcement officials cannot be obtained in time to prevent harm to individuals or destruction of property as, for example, in response to a bomb threat where the bomb cannot be located.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- clandestine intelligence activity
- consent
- counterintelligence
- DoD intelligence components
- employee
- foreign intelligence
- foreign power
- Intelligence Community
- international terrorist activities
- law enforcement
- law enforcement authorities
- narcotics production or trafficking
- sabotage
- United States
- United States person

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 such areas constitute public places, and does not include abandoned property left in a public place.

Sec. 3. Policy

DoD intelligence components may not conduct unconsented physical searches within the United States. Assistance may be rendered to the Federal Bureau of Investigation in the conduct of such searches, however, in accordance with sections 2-308 and 2-309 of Executive Order 12036.

DoD intelligence components may conduct unconsented physical searches of United States persons who are outside the United States, or of property of such persons that is located outside the United States, for foreign intelligence or counterintelligence purposes, pursuant to a warrant issued

by a military judge, the approval of the Attorney General, or in emergency circumstances, pursuant to the approval of a designated senior DoD official.

Sec. 4, Procedures

A. Consented Physical Searches. A DoD intelligence component may conduct physical searches under implied or express consent as follows:

1. Express consent. A DoD intelligence component may conduct physical searches of persons or property with the express consent of the person searched or a person with authority over real or personal property. Determinations of authority shall be made by the general counsel of the DoD intelligence component concerned.

2. Entrance to or Exit from Facilities. A DoD intelligence component may conduct physical searches of persons and property as a condition of entrance to or exit from a DoD facility provided --

   (a) notices are posted publicly at the entrances to the facility indicating that consent to personal and property searches is a condition to access to the facility;

   (b) searches of a person are limited to a "pat-down" search designed to locate equipment, documents, or related espionage devices;

   (c) searches of property are limited to that in possession of a person entering or leaving the facility; and

   (d) searches of person or property are not made when the person learns of the search requirement before entering the facility and elects not to enter

3. Contents of United States Government Storage Facilities, Public Records, Lockers, Desks or other Containers. A DoD intelligence component may search the contents of United States government storage facilities, public records, lockers,

desks and other containers on government property subject to the following limitations --

(a) The contents of Defense Department storage facilities and public records may be examined for counter-intelligence purposes, provided the official having control over such records or facilities or superior consents to such examination;

(b) Government furnished lockers, desks or other containers assigned to individual employees may not be examined without the employee's consent except by a supervisor or other person acting for such supervisor and then only to retrieve public records related to the employee's responsibilities or, in the case of the death or illness of the employee, to obtain other materials belonging to the employee for delivery to a person acting on behalf of the employee. This prohibition does not apply where employees are notified in writing that such lockers, desks, or other containers are for official use only and are to remain unlocked or if locked, duplicate keys or combinations are maintained and will be used to conduct searches.

(c) Lockers, desks or other such containers located inside a Defense facility that are not the property of the Government and that are the property of any employee or other person granted access to a Defense facility may not be examined without consent unless such furniture is being removed from the facility by the employee or other person granted access and the facility has posted notices a its entrance of the type described in subsection 4(A)(2) above. Personal property used solely in residences within a Defense Department facility may not be examined without consent.

4. Areas, Containers, Objects, Vehicles and Other Property not on or Constituting Government Property. A DoD intelligence component may not conduct physical searches of property that is not Government property or that is not located on Government property without the express written consent of a person with authority over such property. The written consent shall include a statement concerning the purpose of search, the specific places, things or vehicle(s) to be searched, the right of the individual not to consent and shall be signed by a person with authority over the property.

5. Persons Not Employees. A DoD intelligence component may not conduct physical searches of persons who are not employees of such components or persons who have not been granted access to facilities or information of such components except for counterintelligence purposes related to the protection of personnel or facilities and then only with the express written consent of the individual to be searched. The written consent shall include a statement concerning the purpose of the search, the degree to which the body of the person will be searched, the right of the individual not to consent and shall be signed by the individual to be searched.

B. Physical Searches Under Implied Consent. A DoD intelligence component may search containers entrusted to a person under circumstances where there is no expectation of privacy with respect to examination of the contents of the container by that person. These searches must be conducted with the consent of the person to whom the container has been entrusted. This search permits the exmination of pouches, packages or envelopes carried by carriers if the above standard is met.

C. Unconsented Physical Searches. A DoD intelligence component may conduct physical searches for foreign intelligence and counterintelligence purposes of United States persons who are outside the United States or of property of such persons that is located outside the United States if the search is conducted pursuant to a military warrant, express approval by the Attorney General or, in emergency circumstances, approval of a senior official of the Department of Defense.

1. Physical search pursuant to Attorney General approval. A DoD intelligence component may conduct a physical search of a United States person who is outside the United States or of the property of a United States person that is located outside the United States if the search is approved by the Attorney General. Requests for approval will be forwarded to the Attorney General through the DoD General Counsel. Each request shall include:

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

   (b) A statement of facts supporting a finding that:

      1. There is probable cause to believe the United States person against whom the search is directed 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 activites, or who conspires with, or knowingly aids and abets such a person engaging in such activities;

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

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 is not enough to bring that person under this subsection (c.) absent evidence that the person is taking directions from, or acting in knowing concert with, the foreign power.

2. Significant foreign intelligence or counterintelligence is likely to be obtained as a result of the search;

3. The significant foreign intelligence or counterintelligence expected to be obtained could not be obtained by less intrusive means.

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

(d) 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.

2. Physical search in emergency situations. A DoD intelligence component may conduct a physical search of a United States person who is outside the United States or of the property of a United States person that is located outside the United States in emergency situations under the following limitations:

(a) Senior officials of the Department of Defense designated in Section 5(b) may authorize physical search in emergency situations when securing the prior approval of the Attorney General is not practical because --

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

(ii) a person's life or physical safety is reasonably believed to be in imminent danger, or

(iii) there is an immediate threat of destruction of government property and local military or other appropriate law enforcement authorities cannot be notified or reach the scene in time to prevent the harm.

(b) The senior official authorizing a physical search shall make a finding (unless a person's life is in immediate danger) that the requirements of subsection 4(C)(1)(b) are met, there is no breaking or nonconsensual entry of real property and any container to be searched as in the lawful custody of the United States. This finding need not be in writing.

(c) The senior official shall notify the DoD General Counsel promptly and the Attorney General shall be notified by the DoD General Counsel as soon as possible of the nature of the search, the circumstances surrounding its authorization, and the result thereof.

D. Cooperation with physical searches by the FBI.

Employees of a DoD intelligence component may cooperate with and assist in physical searches conducted by the Federal Bureau of Investigations only as follows:

1. Foreign intelligence. When a DoD intelligence component identifies a requirement for an unconsented physical search within the United States that is related to foreign intelligence, such a requirement shall be submitted in writing to the Director of the Federal Bureau of Investigation. Employees of DoD intelligence components may not participate with the FBI in the conduct of an authorized unconsented physical search, but may be present and assist the FBI in identifying articles of interest or render technical assistance with respect to foreign intelligence collection equipment.

2. Counterintelligence. When a DoD intelligence component identifies a requirement for an unconsented physical search within the United States that is related to counterintelligence, such a requirement shall be submitted in writing to the Director of the Federal Bureau of Investigation. Employees of DoD intelligence components may not participate with the FBI in the conduct of an authorized unconsented physical search but may be present and assist the FBI in identifying articles of interest or render technical assistance with respect to the analysis and exploitation of material and equipment identified for purposes of --

   (a) protection of personnel or facilities of any agency within the Intelligence Community;

   (b) investigation or preventation of clandestine intelligence activities by foreign powers;

(c) investigation or prevention of narcotics production or trafficking; or

(d) investigation or prevention of international terrorist activities.

3. Other. Expert personnel provided to the FBI in accordance with Procedure 21 may participate in unconsented physical searches as a part of their duties with the FBI.

E. Cooperation with physical searches by foreign officials. Employees of DoD intelligence components may not participate with foreign officials in the conduct of an unconsented physical search not conducted pursuant to these procedures but may be present and assist foreign officials in identifying articles of interest or render assistance with respect to foreign intelligence collection equipment.

Sec. 5. Authority to request physical searches

A. Requests for approval of unconsented physical searches under subsections 4(C)(1) and (2) must be authorized by:

1. The Secretary or the Deputy Secretary of Defense;

2. The Secretary or the Acting Secretary of a Military Department,

3. The Director of the National Security Agency; or

4. The Director of the Defense Intelligence Agency.

B. Authorization for physical searches under subsection 4(B)(3) may be granted by:

1. Any civilian Presidential appointee;

2. Any General or Flag officer; or

3. The head of a DoD intelligence component.

C. Cooperation with physical searches conducted by the FBI may be authorized by the head of any DoD intelligence component or a designee.

Date of Attorney General approval: GBB 8/15/75

Date of Secretary of Defense approval: _____

PROCEDURE 12: MAIL SEARCHES AND SURVEILLANCE

Sec. 1. Applicability and Scope

This procedure implements section 2-205 of Executive Order 12036, ref. (a). It applies to the opening of mail or examination of envelopes in United States postal channels and 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. This procedure does not apply to:

- opening of mail or examination of envelopes for law enforcement purposes;
- opening or examining mail with the consent of the sender or the addressee;
- activities related to the DoD Military Customs Inspection Program conducted under DoD Directive 5030.49, ref. (h); or
- opening or examining mail outside the United States to or from persons who are not United States persons.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure.

- consent
- counterintelligence
- Dod intelligence components
- foreign intelligence
- intelligence
- law enforcement
- United States
- United States person

Mail within United States postal channels includes mail originated in the United States and mail within APO or FPO channels. It also includes mail originating out-

side the United States once it comes within the United States and is handled by the Postal Service regardless of the nationality or status of the sender or recipient.

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 for the purpose of delivery of mail or administration of the postal service.

Sec. 3. Policy

Mail within the United States postal channels or mail to or from United States persons that originated in United States postal channels is not opened or examined by DoD intelligence components except in rare circumstances where significant foreign intelligence or counterintelligence is involved and except as permitted under applicable statutes and regulations.

Sec. 4. Procedure

A. Department of Defense intelligence components may open mail within United States postal channels only pursuant to a judicial warrant in accordance with applicable law. Requests for such a warrant shall be approved and submitted to the Attorney General by the DoD General Counsel.

B. Department of Defense intelligence components may open mail to or from United States persons that is found outside United States postal channels only pursuant to approval by the Attorney General. Requests for such approval shall be submitted to the Attorney General by the DoD General Counsel.

C. The following officials may request approval to open mail --

1. The Secretary and Deputy Secretary of Defense; and

2. The Secretaries and Acting Secretaries of the Military Departments.

D. Department of Defense intelligence components may utilize mail covers --

1. within the United States consistent with postal regulations.

2. outside the United States if consistent with applicable status of forces agreements, or where there are no such agreements, if consistent with the law of the jurisdiction where the activity takes place.

E. Department of Defense intelligence components may request postal authorities to inspect the contents of any second-, third-, or fourth-class mail within the United States and may inspect such contents outside the United States for intelligence purposes.

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 13: PHYSICAL SURVEILLANCE

Sec. 1. Applicability and Scope

This procedure implements section 2-206 of Executive Order 12036, ref. (a), and applies to the physical surveillance of United States persons by DoD intelligence components. This procedure does not apply to:

- physical surveillance of persons who are not United States persons;
- physical surveillance for law enforcement;
- surveillance activities that use electronic of mechanical devices such as television cameras, movie cameras, beepers or telescopic microphones in circumstances in which a warrant would be required in the criminal context; those are governed by Procedures 4, 5, and 10;
- activities involved in physical searches; those are governed by Procedure 11;
- undisclosed participation in organizations; that is covered by Procedure 14;
- routine surveillance of open areas, parking lots, corridors, entrance and exits, safes and vaults, restricted access areas and other areas where classified information is stored;
- use of uniformed guards to control access to the premises or portions of the premises of DoD intelligence components; or
- physical surveillance conducted as a part of a military training exercise where the subjects are participants in the exercise.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- consent
- contact
- contractor
- counterintelligence
- counterintelligence investigations
- DoD intelligence components
- electronic surveillance
- employee
- foreign intelligence
- foreign power
- intelligence method
- intelligence source
- international terrorist activities
- law enforcement
- lawful investigation
- member of a military service
- narcotics production or trafficking
- physical security
- physical security investigation
- physical surveillance
- reasonable belief
- United States
- United States person

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

- There is a "systematic and deliberate observation" of a person when the observation is made over a period of time with the purpose of keeping a person under observation. Incidental observations made in the course of a surveillance are not included.

- A communication is "nonpublic" when it is not a public broadcast and when it is made under circumstances in which there is a reasonable

expectation that no one will hear it other than the person or persons to whom the communication is directed.

A person is "visibly present" at a conversation if he or she is within plain sight of the person doing the communicating. If a person deliberately concealed from view overhears a conversation, that would constitute physical surveillance.

Sec. 3. Policy

DoD intelligence components do not use physical surveillance directed against a United States person unless that technique is necessary to achieve a lawful foreign intelligence or counterintelligence purpose or is a part of a lawful physical security investigation. Physical surveillance within the United States and outside DoD installations is conducted in conformity with the agreement between the Department of Defense and the Federal Bureau of Investigation dated April 5, 1979, Ref. (n).

Sec. 4. Procedures

A. General Criteria for Physical Surveillance. A DoD intelligence component may direct physical surveillance only at certain categories of persons --

1. Within the United States only against --

- employees of the intelligence component;
- contractors of the intelligence component;

- employees of such contractor; and
- members of the military services

Within the United States a DoD intelligence component may conduct physical surveillance only on DoD installations unless such surveillance is directed at a member of the military service or is "hot pursuit," or is otherwise undertaken consistent with Ref. (n).

2. Outside the United States may be conducted against--

- all persons under Subsection 4(A)(1);
- former employees of a DoD intelligence component;
- former contractors;
- former contractor employees;
- civilian persons employed by a non-intelligence component of DoD; and
- persons in contract with a present or former employee or contractor (but only to the extent necessary to identify that person).

B. Physical surveillance for positive foreign intelligence purposes. A DoD intelligence component may conduct physical surveillance:

1. Within the United States, if the surveillance meets the criteria set out in Section 4(A) and is conducted solely for the purpose of identifying a person who is in contact with someone who is the subject of a lawful foreign intelligence investigation. A person is the "subject of" a foreign intelligence investigation if foreign intelligence is sought from or about that person. The person who is the foreign intelligence target may be either a United States person or a foreigner. The information that may be collected about the foreign intelligence target's contact is limited to information necessary to identify that person, including name, address, and employment.

2. Outside the United States, if

   (a) the surveillance meets the criteria in Section 4(B)(1), or

   (b) the person surveilled is reasonably believed to be acting on behalf of a foreign power. An action is taken "on behalf of" a foreign power when it is done to further an activity, capability or intention of a foreign power.

C. Physical surveillance for counterintelligence purposes.

A DoD intelligence component may conduct physical surveillance for counterintelligence purposes if

1. The surveillance is directed at a person who is the subject of a lawful counterintelligence investigation.

A person is the "subject of" a counterintelligence investigation when the investigation has focused on that person's activities.

2. The surveillance is conducted solely for the purpose of identifying a person who is in contact with someone who is the subject of a lawful counterintelligence investigation.

The information that may be collected about the United States person who is in contact with the counterintelligence target is limited to information necessary to identify that person, including name, address, employment, and security clearance.

Physical surveillance conducted for counterintelligence purposes within the United States must also meet the criteria set out in Section 4(A).

D. Physical surveillance for protection of intelligence sources and methods. A DoD intelligence component may conduct physical surveillance for the purpose of protecting a foreign intelligence or counterintelligence source or method from unauthorized disclosure. Physical surveillance for this purpose may be conducted:

1. Within the United States, only if the surveillance meets the criteria set out in Section 4(A) and only against:

(a) A present employee of a DoD intelligence component;

(b) A present contractor of a DoD intelligence component;

(c) A present employee of a present contractor of a DoD intelligence component; or

(d) A member of a military service.

2. Outside the United States, if the surveillance meets the criteria set out in Section 4(A) above and is conducted against:

(a) Any person covered by subsections 4(D)(1)(a)-(d) above;

(b) A former employee of a DoD intelligence component;

(c) A former contractor of a DoD intelligence component; or

(d) A present or former employee of a present or former contractor of a DoD intelligence component;

(e) A person who is in contact with someone described in subsection 4(D)(2)(a), (b), or (c) above but only to the extent necessary to identify that person, including name, address, employment and security clearance.

E. Physical surveillance for physical security purposes. A DoD intelligence component may conduct physical surveillance for the purpose of protecting the physical security of the installations of DoD components. The surveillance must be conducted as a part of a lawful physical security investigation and must meet the following criteria:

1. The surveillance is conducted against persons who are specified in Subsection 4 (D)(1) and (2) above;

2. The surveillance is conducted against persons who are --

   (a) discovered on a Defense or intelligence installation without authorization;

   (b) discovered in a portion of an installation under circumstances such that there is a reasonable belief that such person is violating or is about to violate laws or regulations relating to the protection of classified information; or

   (c) reasonably believed to be engaging in activities that are directed at or will result in unauthorized entry onto or the compromise of the security of an installation.

2. Information may be collected regarding the person's --

   (a) identification;

   (b) location; and

   (c) activities, intentions, and capabilities with respect to breaching the physical security of the installations.

F. Physical surveillance of persons engaging in international terrorist activities. A DoD intelligence component may conduct physical surveillance outside the United States of a United States person who is reasonably believed to be engaged in international terrorist activities. A person is "engaged in" an activity if that person has taken some action in furtherance of the activity or is in contact with a person or organization that has taken such action under circumstances that support a reasonable belief that action by that person in furtherance of the activity will follow.

G. Physical surveillance of persons engaging in narcotics production or trafficking. A DoD intelligence component may conduct physical surveillance outside the United States of a United States person who is reasonably believed to be engaged in narcotics production or trafficking. Information collected should be limited to the person's identification; location; and activities, intentions, capabilities and associates with respect to narcotics production or trafficking.

H. Approval of physical surveillance. Physical surveillance other than for purposes of identification must be authorized by the head of the intelligence components or one of two designated senior officials. Physical surveillance for identification purposes may be authorized by a field supervisor.

Date of Attorney General approval: GBB 8/15/79

Deat of Secretary of Defense approval: _____

PROCEDURE 14. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

Sec. 1. Applicability and Scope

This procedure implements Section 2-207 of Executive Order 12036, ref. (a), and applies to participation by employees of DoD intelligence components in any organization within the United States or that is primarily composed of United States persons when participation is on behalf of any entity of the intelligence community. These procedures do not apply to:

- the undisclosed participation by DoD employees acting on behalf of Department of Defense investigative organizations when the participation is for law enforcement purposes and is conducted under the provisions of DoD Directive 5200.27, ref. (l);
- contracting or other arrangements for goods and services; that is governed by Procedure 15; or
- assignment of employees of DoD intelligence components to other agencies; that is governed by Procedure 18.

Undisclosed participation in organizations not affiliated with the Department of Defense by employees of DoD intelligence components is exempted from the requirements of DoD Directive 5200.27, Ref. (l).

Sec. 2. Definitions and Interpretations

The definitions of the following terms, set out in enclosure 3, are applicable to this procedure:

- contact
- counterintelligence
- cover
- DoD intelligence component
- employee

- foreign intelligence
- foreign power
- intelligence community
- international terrorist activities
- law enforcement
- lawful investigation
- reasonable belief
- United States
- United States person

Participation in this context means taking one or more of the following actions with respect to an organization -- acquiring membership, attending meetings not open to the public, contributing to the work of the organization, or providing funds to the organization other than in payment for goods or services. Participation is covered by this procedure if it occurs within the United States.

Participation is on behalf of an agency within the intelligence community when the employee has been directed to participate as a part of his or her work assignment or when any information, contacts, cover, or work product of the participation is intended for delivery to or for the benefit of such agency. Participation for personal purposes of increasing an employee's store of knowledge, personal associations or social contacts or for the benefit of an employee's extra-curricular interests is not covered by this procedure. A person will not be acting on behalf of an agency within the intelligence community if he is not paid by the agency, if he is not in any way controlled by the agency, and if he does not undertake any action that constitutes participation at the direction or request of the agency.

An organization is primarily composed of United States persons when one-half or more of the members, participants or employees of the organization are United States persons. This is a rough rule of thumb and doubts about total members or numbers of United States persons should be resolved in favor of the additional protection accorded organizations that are substantially composed of United States persons. An action is taken on behalf of a foreign power when it is done to further an activity, capability or intention of a foreign power. An organization acts only through its members, officers, employees and agents. The act of a person may be attributed to the organization when it was done at the direction of or for the benefit of the organization.

Sec. 3. Policy

Employees of Department of Defense intelligence components do not participate in organizations within the United States without disclosing their affiliation with the Department and with the intelligence component unless the participation is for personal and not official purposes or unless participation without disclosure has been approved by the Deputy Under Secretary of Defense (Policy Review).

Sec. 4. Procedures

A. Undisclosed Participation on Behalf of the FBI. The undisclosed participation of an employee of a DoD intelligence component in an organization within the United States, as part

of a lawful investigation or operation by the Federal Bureau of Investigation must be requested in writing by the FBI and approved by the Deputy Under Secretary or Defense (Policy Review).

B. Undisclosed Participation in an Organization Not Primarily Composed of United States Persons and Reasonably Believed to be Acting on Behalf of a Foreign Power. Undisclosed participation of this type shall be requested and approved in the following manner:

1. Authority to approve such participation shall be limited to the Deputy Under Secretary of Defense (Policy Review) who shall find that such non-disclosure is essential for accomplishment of a lawful purpose. Such finding shall be subject to review by the Attorney General.

2. Authority to request such participation shall be limited to the Secretaries and Under Secretaries of the Military Departments.

3. Requests for authority for such participation shall include a statement of facts sufficient to show that the organization concerned is not primarily composed of United States persons, and is reasonably believed to be acting on behalf of a foreign power. Such requests shall also show that the FBI has concurred in the participation being requested.

C. Undisclosed Participation for Limited Foreign Intelligence Purposes. Employees of DoD Intelligence components may participate in the following activities without disclosure of affiliation with an intelligence component.

1. Participation in meetings, conferences, exhibitions, trade fairs, and similar gatherings sponsored by organizations which are open to the public and which are designed to enhance the skills, knowledge or capabilities of the employee.

2. Participation in technical or professional seminars, associations, conferences, workshops, symposiums and other meetings sponsored by technical organizations although such education and training could be applied to foreign intelligence uses

3. Membership in an organization solely for the purpose of establishing professional or educational credentials.

4. Employees who participate in the activities of an organization under subsection (1), (2) or (3) above may, if requested, identify themselves as Department of Defense employees, or members of a military service or command, without specifying their intelligence affiliation.

D. Participation in Organizations Where Non-Disclosure of Affiliation is Essential to Achieving Lawful Purposes. Undisclosed participation under this subsection shall be approved as follows:

1. Authority to approve such participation shall be limited to the Deputy Under Secretary of Defense (Policy Review) who shall find that such non-disclosure is essential for accomplishment of a lawful purpose. Such finding shall be subject to review by the Attorney General.

2. Authority to request such participation shall be limited to the Secretaries and Under Secretaries of the Military Departments, and the heads of DoD intelligence components.

3. Requests for approval of such participation shall include a statement of facts sufficient to show that such participation is essential to a lawful foreign intelligence purpose. "Lawful foreign intelligence purposes" are limited to --

(a) Participation to establish contact with a potential source of foreign intelligence or a potential source of assistance in foreign intelligence activities;

(b) Participation to establish contact with someone who is a target of foreign intelligence;

(c) Participation outside the United States to collect foreign intelligence, but not to acquire information concerning the organization in which the individual is participating;

(d) Participation within the United States to collect foreign intelligence from cooperating sources, otherwise unobtainable, where such sources would be lost if disclosure of the relationship with the intelligence component were made, provided that such participation has been approved by the Special Coordination Committee of the National Security Council, and the organization is primarily composed of persons subject to the Uniform Code of Military Justice, 10 U.S.C. § 802, Art. 2(1) through (10); or

(e) Participation to establish cover necessary to protect the security of foreign intelligence.

(f) Participation in organizations which permit government employees to so participate in their official capacity.

4. Participation may not be undertaken for the purpose of influencing the activity of the organization or its members.

5. Approval under these procedures shall specify the duration of participation (not to exceed 12 months) and include provisions to ensure that the participation is limited to approved purpose.

E. Disclosure of Participation. Unless nondisclosure is approved under this procedure, all participation in organizations by employees of DoD intelligence components on behalf of such components shall be disclosed to an executive officer of the organization or to the official in charge of membership, attendance, or the records of the organization, if disclosure of affiliation is normally required of all members or participants in such organization.

Date of Attorney General approval: FEB 9 1979

Date of Secretary of Defense approval: _____

PROCEDURE 15. CONTRACTING FOR GOODS AND SERVICES

Sec. 1. Applicability and Scope

This procedure implements Section 2-303 of Executive Order 12036, ref. (a), and applies to contracting or other arrangements for the procurement of goods and services by DoD intelligence components within the United States. This procedure applies to contracting with or procurement from corporations, other commercial organizations, academic institutions and other private institutions or individuals. This procedure does not apply to:

- contracting outside the United States even if the contractor is a United States person and the goods and services are to be delivered wholly or in part within the United States; or
- contracting with government entities.

Sec. 2. Definitions

The definitions of the following terms, set out in enclosure 3, are relevant to this procedure:

- availblable publicity
- contractor
- commercial organization
- corporation
- cover
- DoD intelligence components
- intelligence
- intelligence method
- intelligence source
- intelligence community
- United States
- United States person

A United States academic institution, in this context, is an institution that is a United States person and that is operated or holds itself out as a degree-granting institution. Both public and private academic institutions are treated the same for this purpose.

The term "private institution" includes associations, organizations and other entities that have no government affiliation and that are not corporations, commercial organizations, or academic institutions.

A contract is with an individual rather than the organization with which the individual is affiliated when it is in writing, only the name of the individual appears as a contracting party, and no part of the consideration is specified in the contract as payable to the organization.

Contracting "by or for" a DoD intelligence component includes placing with or accepting from other agencies within the Intelligence Community requests to procure goods and services from corporations, commercial organizations, and private institutions in order to protect from disclosure sensitive intelligence activities, facilities, or relationships.

Contracting or other procurement arrangements are "within the United States" when the contract is entered at a place within the United States. The contract may recite that it was entered within the United States and that will be dispositive for purpose of this procedure.

Sec. 3. Policy

The Department of Defense discloses the maximum amount of information about the sponsorship of contracts made within the United States to obtain goods and services that is consistent with the need for protection of intelligence activities or intelligence sources and methods from disclosure.

Sec. 4: Procedure

A. Academic institutions. Contracting by or for DoD intelligence components with United States academic institutions may be done only in compliance with the following requirements:

1. No DoD intelligence component may enter a contract for goods or services with an academic institution unless, 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. No DoD component may enter a contract with an academic institution for the provision of goods and services to be used primarily by or for the principal benefit of a DoD intelligence component unless prior to the making of the contract, the DoD component has disclosed to appropriate officials the fact of sponsorship by a DoD intelligence component.

3. Disclosure is adequate if --

   (a) the name of the DoD intelligence component appears on the face of the contract as a contracting party or as a component authorized to take delivery of goods or services under the contract;

   (b) there is appended to the contract a classified annex stating that the goods or services to be delivered under the contract are for the use of a DoD intelligence component; or

   (c) the contracting officer or other appropriate officer of the academic institution is informed orally of sponsorship of a DoD intelligence component and a written memorandum describing the information given to the officer and the time and place of the oral communication is made a part of the contract files of the DoD intelligence component.

Under subsections 4(A)(3)(b), and (c) above, disclosure need not include the identity of the specific DoD intelligence component that will receive the goods or services.

B. Commercial organizations and private institutions. Contracting by or for a DoD intelligence component with corporations, commercial organizations or private institutions may be done only if at least one of the following criteria is met:

1. There has been disclosure, prior to the making of the contract, of the fact of sponsorship by a DoD intelligence component. Disclosure is adequate if one of the criteria of subsection 4(A)(3) is met.

2. The contract is for written material that is available publicly, such as books, magazines, and journals available to the general public, routine goods or services for office use such as telephone, heat and light; and office equipment and supplies available to the general public, such as typewriters, furniture, data processing equipment, interior or exterior maintenance services; and routine supplies or services for vehicle operation and maintenance.

3. The contract is for routine goods and services such as credit cards, car rentals, travel, lodging, meals and other items incident to approved intelligence activities.

4. There is 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 Assistant Secretary of Defense (Communications, Command, Control and Intelligence) that the sponsorship of a DoD intelligence component needs to be concealed. That determination must be supported by findings that--

(a) concealment is necessary to maintain cover or proprietary arrangements,

(b) the cover or proprietary arrangements to be maintained are essential to the intelligence activities of a DoD component, and

(c) the activities of the DoD component for which cover or proprietary arrangements are used are authorized intelligence activities.

Determinations may be made for categories of contracts.

C. Individuals. Contracting by or for a DoD intelligence component with an individual person may be done only if there has been oral or written disclosure of the sponsorship by the intelligence component or a determination under subsection 4(B)(4) has been made.

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

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

PROCEDURE 16. PROVISION OF ASSISTANCE BY EXPERT PERSONNEL TO LAW ENFORCEMENT AUTHORITIES

Sec. 1. Applicability and Scope

This procedure implements Sections 2-309(c) of Executive Order 12036, ref. (a), and applies to the provision of assistance by expert personnel from DoD intelligence components to law enforcement authorities within the United States. These procedures do not apply to:

- employees of DoD intelligence components who are assigned law enforcement duties when carrying out such duties; or
- activities of intelligence components outside the United States

Sec. 2: Definitions

The definitions of the following terms, set out in enclosure 3, are applicable to these procedures.

- DoD intelligence components
- employee
- expert personnel
- law enforcement
- law enforcement activities
- law enforcement authorities
- state
- United States

Sec. 3. Policy

DoD intelligence components may provide expert personnel to assist law enforcement authorities in other departments or agencies

of the United States Government, or, if lives are endangered, such assistance may be provided state and local law enforcement authorities. Such support shall be limited to those persons with particular skills which are otherwise not readily available to such authorities but are necessary for performing a law enforcement function.

Sec. 4. Procedures

A. Provision of Expert Personnel to Federal Law Enforcement Authorities. Provision of expert personnel to any federal law enforcement agency may be made only pursuant to a request from the head of such agency. The participation of a DoD intelligence component in response to such a request shall be limited in the following respects:

1. The only personnel to be provided are experts who can assist in specialized technical, systems or logistics assignments;

2. The assignment of expert personnel to a federal law enforcement agency is accomplished in compliance with the requirements of DoD Directive 1000.17, ref. (f), and Procedure 14;

3. Such personnel are not used by the requesting federal law enforcement agency to participate actively in or direct the apprehension of persons violating the criminal laws of the United States;

4. The requirements of the Posse Comitatus Act, ref. (c), are met;

5. No assignment exceeds 90 days without the written approval of the Secretary of Defense or a designee; and

6. The requesting federal law enforcement agency does not assign such personnel to duties other than those set out in the memorandum required by Section D(6)(c)(1) of DoD Directive 1000.17, ref. (f).

B. Provision of Expert Personnel to State and Local Law Enforcement Authorities. Expert personnel may be provided by DoD intelligence components to state and local law enforcement authorities only when lives are endangered and only pursuant to a request by the head of such authority. Under these circumstances expert personnel may be provided to such agency provided participation in law enforcement activities is limited as follows:

1. Only personnel with technical skills not readily available to such law enforcement authorities which can be utilized to prevent death or serious injury may be provided;

2. Provision of such personnel will be limited to that necessary to prevent the death or serious injury that is threatened, but in no case shall such assistance be provided for more than 72 hours;

3. Such personnel are not used to apprehend persons who are suspected of committing, or who are about to commit, a crime; or

4. Use of such personnel does not violate the Posse Comitatus Act, ref. (c).

C. Emergency Assistance. In emergency situations, where life is endangered, the request required in subsection A or B of this section may be oral, provided that it is reduced

to writing and submitted in accordance with this section within 72 hours. Where life is endangered, doubt as to the legality and propriety of the requested assistance under this procedure should be resolved in favor of providing the assistance.

D. Notice of Assistance. Notice of the provision of expert personnel to law enforcement authorities pursuant to this procedure shall be given to the General Counsel, Department of Defense, within five days after such assistance has been provided.

Date of Attorney General approval: GBB 8/15/79

Date of Secretary of Defense approval: _____

(Encl. 3)
July 12, 1979

DEFINITIONS

1. Administrative purposes. Information is stored for "administrative purposes" when it is retained solely because it relates to one or more of the following: Contracting, building maintenance, construction, fiscal matters, internal accounting procedures, disciplinary matters, public affairs, legislative affairs, and other matters not related to intelligence or security.

2. Agent of a foreign power, means --

(1) any person other than a United States person, who --

(a) acts in the United States as an officer or employee of a foreign power, or as a member of group engaged in international terrorism or activities in preparation therefor;

(b) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who --

(a) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(b) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(c) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power; or

(d) knowingly aids or abets any person in the conduct of activities described in subparagraph (a), (b) or (c) or knowingly conspires with any person to engage in activities described in subparagraphs (a), (b), or (c).

3. Available publicly means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully b 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.

4. Clandestine intelligence activity means an activity conducted for intelligence purposes or for the purpose of affecting political or governmental processes by or on behalf of a foreign power in a manner designed to conceal from the United States Government the nature or fact of such activity or the role of such foreign power, and any activity conducted in support of such activity.

5. Collecting agency means, with respect to information, the department or agency that collects the information.

6. Commercial organization means an organization that is not incorporated and that operates or holds itself out as a business enterprise usually, but not necessarily, for the purpose of making a profit. This term covers business partnerships, companies, associations, and sole proprietorships. Organizations that use the word "Co.," and other common commercial designations may be treated as commercial organizations for purposes of these procedures. Some charitable, literary, and social organizations conduct incidental operations for profit. Not every activity designed to make a profit will qualify an entity as a commercial organization. Nor will any incidental charitable, literary or social activity remove an organization from that category of commercial organization. The determination is made by assessing the nature of the organization.

7. Communications security means protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such telecommunications.

8. Consent is 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).

9. Contact. Several sections in the procedures permit collection of information about a United States person who is in "contact" with someone else. Contact in this context means a reasonable belief that there has been direct communication between two persons. "Reasonable belief" should be determined in accordance with guidance under the definition of that term in this enclosure.

10. Contractor means a person or organization that provides goods or services directly to a DoD intelligence component. A person or organization is a contractor of a DoD intelligence component if the work done by the contractor is under the direction of or solely for the use of a DoD intelligence component regardless of the source of funds for payment to the contractor.

11. Corporation means an organization incorporated in the United States under federal, state or local law. The fact and place of incorporation is determinative. Entirely foreign ownership does not disqualify an organization for treatment as a corporation under these procedures. Use of the words "Inc.," or "Corp.," in the title of an organization is sufficient for it to be treated as a corporation for purposes of these procedures.

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

13. Counterintelligence investigation includes inquiries and other activities undertaken to determine whether a particular U.S. person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other clandestine intelligence activities, sabotage, international terrorist activities

or assassinations and to neurtralize such acts. A counter-intelligence investigation, for purposes of these procedures, does not include counterespionage operations undertaken against foreign powers.

14. Cover means an arrangement to conceal the true identity of persons acting for or on behalf of an entity of the intelligence community, or the relationship of such persons to such entities.

15. 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 for Intelligence, Air Staff;
(g) The Army Intelligence and Security Command;
(h) The Naval Intelligence Command;
(i) The Air Force Intelligence Service;
(j) The counterintelligence elements of the Naval Investigative Service;
(k) The counterintelligence elements of the Air Force Office of Special Investigations;
(l) The 650th Military Intelligence Group, SHAPE; and
(m) The intelligence units of the Military Departments that support Unified or Specified Commands.

16. 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 or the use of pen register equipment.

17. Electronic communications equipment means electronic equipment capable of undetected interception of electronic or oral communications. It does not include equipment designed for use only in the transmission of communications. It does not include equipment designed to determine the direction and location of radio transmitters such as radio direction-finding equipment.

18. Employee means a person employed by, assigned to, or acting for an agency within the Intelligence Community. It includes military personnel assigned to an intelligence component. It includes persons on leave status or other arrangement for absence from duties except permanent severance. It includes persons who are consultants, members of an advisory board, employees of a nonappropriated fund activity associated with a Defense intelligence agency, employees of an agency credit union, or commercial enterprise located within agency premises, or gratuitous servants assigned to duty with the DoD intelligence component. See DoD Directive 5200.25 and 5210.26.

19. Expert personnel means persons who are employees of a DoD intelligence component and who possess a specialized technical knowledge or skill.

20. 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.

21. Foreign power means 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.

22. Intelligence means foreign intelligence and counterintelligence.

23. Intelligence Community and agency or agencies within the Intelligence Community refer 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 military services, the Federal Bureau of Investigation (FBI), the Department of the Treasury, the Department of Energy; and the Drug Enforcement Administration (DEA); and

(g) The staff elements of the Office of the Director of Central Intelligence.

24. Intelligence method means any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

25. Intelligence product means the estimates, memoranda and other reports produced from the analysis of available information.

26. Intelligence source means a person or technical means that provides intelligence.

27. International terrorist activities means any activity or activities which:

(a) involve killing, causing serious bodily harm, kipnapping or violent destruction of property, or an attempt or credible threat to commit such acts; and

(b) appear intended to endanger a protectee of the Secret Service or the Department of State or to further political, social or economic goals by intimidating or coercing a civilian population or any segment thereof, influencing the policy of a government or international organization by intimidation or coercion, or obtaining widespread publicity for a group or its cause; and

(c) transcend national boundaries in terms of the means by which it is accomplished, the civilian population, government, or international organization it appears intended to coerce or intimidate, or the locale in which its perpetrators operate or seek asylum.

28. Law enforcement means detecting violations of criminal law and identifying or apprehending persons who have violated the criminal law so that they may be prosecuted for other crimes. In this context the criminal law includes federal statutes, federal regulations and the Uniform Code of Military Justice.

29. Law enforcement activities means the activities undertaken in order to detect violations of law or to locate and apprehend persons who violate the law. These include activities to enforce the Uniform Code of Military Justice. Some DoD intelligence components carry out both law enforcement and intelligence functions. The same personnel may be used to carry out both functions. They are engaged in law enforcement activities when the purpose of the activity is detecting violations of criminal law and identifying or apprehending persons who have violated the criminal law. They are engaged in intelligence activities when the purpose of the activity is to obtain or produce foreign intelligence or counterintelligence. There is one exception to this distinction between the two functions. Espionage investigations could be seen as serving both law enforcement and counterintelligence purposes. But for purposes of these procedures, all espionage investigations, even if undertaken under circumstances where criminal prosecution is a possible outcome, which constitute part of the foreign counterintelligence program of the Department of Defense, shall be considered as counterintelligence activities and not law enforcement activities. Some activities of DoD intelligence components undertaken in order to collect foreign intelligence and counterintelligence will produce information that is useful in detecting violations of law or locating and apprehending persons who violate the law. These intelligence and counterintelligence activities do not thereby become law enforcement activities.

30. Law enforcement authorities include military police, local police, state police, the Federal Bureau of Investigation, the Executive Protective Service, and special police employed by federal, state and local government agencies. The Army Intelligence and Security Command, the Naval Investigative Service, and the Air Force Office of Special Investigations each have counterintelligence responsibilities and law enforcement responsibilities under the Uniform Code of Military Justice. When engaged in law enforcement responsibilities, these components are law enforcement authorities. Components that supervise these military investigative authorities, when they are engaged in law enforcement responsibilities, are also law enforcement authorities.

31. Lawful investigation. An investigation qualifies as a lawful investigation if it is conducted by a DoD component that has authorization to conduct the particular type of investigations (for example, counterintelligence, physical security, communications security) and if the techniques used to further the investigation are lawful. The term does not include an investigation of "leaks" directed against a particular individual and using techniques governed by procedures in enclosure 1 when the purpose of the investigation is to determine the individual's source of information. Such inquiries may be undertaken only if there is a reasonable belief that the individual who has the information is personally engaged in activities that may involve a violation of law or Department of Defense regulations applicable to that individual.

32. Member of a military service means a person currently serving in the United States Army, Navy, Air Force, Marine Corps, or an active reserve or National Guard component thereof, including the United States Coast Guard when the Coast Guard is operating as a part of the Department of the Navy.

33. Narcotics production or trafficking means activities outside the United States to produce or deal in narcotics or other substances controlled under the Controlled Substances Act of 1970, Pub. L. No. 91-613, title II, 84 Stat. 1242 (codified in scattered sections of 15, 31, 42 U.S.C.).

34. Personnel security means the protection resulting from measures designed to insure that persons employed 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 insure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

35. Personnel security investigation means:

(a) An inquiry into the activities of a person granted access to intelligence or other classified information; or a person who is to be granted access to intelligence or other classified information, including persons who are granted access to facilities of Defense 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) investigations conducted when it is learned that a DoD employee or member of a military service has relatives or close associates abroad; and

(d) the collection of information about or from military personnel in the course of tactical training exercises for security training purposes.

36. Physical security means the protection resulting from physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard against espionage, sabotage, damage and theft.

37. Physical security investigation means an inquiry into or survey of the effectiveness of security controls and procedures established to protect classified information, equipment or property. Security controls or procedures include physical controls established around the perimeter of a facility, building or office; controls established with respect to the equipment or other property; procedures governing access by visitors and procedures related to access to intelligence information by persons other than employees; procedures and controls related to the safe storage and transmittal of classified information including cryptographic information, materials and equipment; procedures limiting employee access to classified information on a need-to-know basis; and

procedures and controls related to the disposal of classified equipment and wastes. Physical security investigation includes inquiries and other actions undertaken against United States persons who are present upon, or are in physical proximity to, an installation or facility of a DoD component and who are reasonably believed to pose a clear threat to the physical safety of personnel, equipment, information, or activities of such component.

38. Physical surveillance means an unconsented, systematic and deliberate observation of a person by any means on a continuing basis, or unconsented acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance. This definition does not include overhead reconnaissance not directed at specific United States persons.

39. Reasonable belief. Several of these procedures require an assessment of "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. Reasonable belief also depends on the circumstances in which it is formed. In emergency situations, a reasonable belief can be supported by the facts at hand and the need to take action immediately to avoid imminent harm.

40. Sabotage means any activity that involves a violation of chapter 105 of title 18, United States Code, or that would involve such a violation if committed against the United States.

41. Signals intelligence means a category of intelligence including communications intelligence, electronic intelligence, and instrumentation intelligence, either individually or in combination.

(a) Communication intelligence means information derived from foreign communications by other than the intended recipients.

(b) Electronics intelligence means information derived from electromagentic radiations other than communications emanating from foreign sources other than nuclear detonations or radioactive sources.

(c) Instrumentation intelligence means information derived from the collecting and processing of foreign telemetry, beaconry, nonimagery infrared and coherent light signals.

42. State means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the Virgin Islands, American Samoa, Wake Island, Midway Island, Guam, Palmyra Island, Johnston Atoll, Navassa Island, and Kingman Reef.

43. United States, when used to describe a place includes the terrorities of the United States.

44. United States person means a citizen of the United States, an alien lawfully admitted for a permanent residence, an unincorporated association organized in the United States or substantially composed of United States citizens or aliens admitted for permanent residence, or a corporation incorporated in the United States.

45. Wire communication means any communication while it is being carried by a wire, cable or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

Date of Attorney General Approval GBS 5/15/79

Date of Secretary of Defense Approval _____