NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

20 October 1980

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE (USSID)

18

LIMITATIONS AND PROCEDURES IN SIGNALS INTELLIGENCE OPERATIONS OF THE USSS (U)

LETTER OF PROMULGATION

(U) This directive prescribes policies and procedures, and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights and privacy of U.S. persons.

(U) This USSID supersedes USSID 18, dated 26 May 1976, and is effective upon receipt.

B. R. INMAN
Vice Admiral, U.S. Navy
Director, NSA/Chief, CSS

[redacted]

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 20 OCTOBER 2010

SECURITY CLASSIFICATION

CHANGE REGISTER

CHANGE			ENTERED	
NO.	DATE	AUTHORITY (Msg Cite/DTG, Hard Copy (HC), OPSCOMM)	DATE	BY
1	070205Z Apr 81	(para 5.1.b.(2))	9 Apr 81	[redacted]
1	11 Jul 86	Ltr	31 Jul 86	[redacted]
3	20 Apr 88	[redacted] 3104-88, 201125Z Apr 88	7 Jul 88	[redacted]

FORM A7093 REV AUG 76 (Supersedes A7093 Nov 72 which is obsolete)

SECURITY CLASSIFICATION

TABLE OF CONTENTS

SECTION 1 - REFERENCES . . . . . PAGE 1

SECTION 2 - PURPOSE AND APPLICABILITY . . . . . PAGE 1

SECTION 3 - DEFINITIONS . . . . . PAGE 2

SECTION 4 - POLICY . . . . . PAGE 9

SECTION 5 - COLLECTION . . . . . PAGE 10

SECTION 6 - PROCESSING . . . . . PAGE 11

SECTION 7 - STORAGE . . . . . PAGE 13

SECTION 8 - DISSEMINATION . . . . . PAGE 14

SECTION 9 - RESPONSIBILITIES . . . . . PAGE 17

SECTION 10 - ACCOUNTABILITY . . . . . PAGE 19

ANNEX A - PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U) 1/

ANNEX B - OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U)

ANNEX C - SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U)

ANNEX D - TEST AND EVALUATION OF ELECTRONIC EQUIPMENT (U)

ANNEX E - COMMUNICATIONS SECURITY (U)

ANNEX F - SEARCH AND DEVELOPMENT OPERATIONS (U)

ANNEX G - [redacted]

ANNEX H - TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SIGINT COLLECTION EQUIPMENT (U)

ANNEX I - SAMPLE CONSENT FORMS (U)

1/ Issued Separately to Selected Recipients.

USSID 18
20 October 1980

LIMITATIONS AND PROCEDURES IN SIGNALS INTELLIGENCE OPERATIONS OF THE USSS (FOUO)

SECTION 1 - REFERENCES

1.1. (FOUO) References

a. DoD Regulation 5240.1-R.

b. NSA/CSS Directive No. 10-30, dated 24 March 1980.

c. Executive Order 12036, United States Intelligence Activities, 24 January 1978.

d. 50 U.S.C. 1801, Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511 (see Annex A).

SECTION 2 - PURPOSE AND APPLICABILITY

2.1. (FOUO) This USSID implements the provisions of DoD Regulation 5240.1-R for the USSS. It prescribes general policy and SIGINT operating policy, and provides procedures and assigns responsibilities to ensure that the SIGINT mission of the National Security Agency/Central Security Service is conducted in a manner that guarantees proper safeguards to the rights and privacy of U.S. persons under applicable law, executive branch directives, internal directives, and policy. The annexes to USSID 18 contain procedures that must be followed for the specialized SIGINT operations and targets to which they pertain. The other policies and procedures in this USSID provide guidance in applying specific restrictions in SIGINT operations to targeting, collection, selection, storage, and dissemination of information, and the maintenance of data bases that may relate to U.S. persons. The policies and procedures herein apply to all elements of the USSS.

[redacted]

SECTION 3 - DEFINITIONS

3.1. [redacted]gent of a foreign power, means -

a. Any person, other than a U.S. person, who -

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

(2) Acts for, or on behalf of, a foreign power that 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;

b. Any person, including a U.S. person, who -

(1) 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;

(2) 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;

(3) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for, or on behalf of, a foreign power; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 3.1.b.(1), 3.1.b.(2), or 3.1.b.(3) or knowingly conspires with any person to engage in such activities; or

c. A U.S. person, residing abroad, who holds an official position in a foreign government or the military forces of a foreign nation and information about whose activities in that position would constitute foreign intelligence.

3.2. (FOUO) 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, has been seen or heard by a casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

3.3. (FOUO) 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.

3.4. ([redacted]) Collection means intentional tasking and/or selection of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

3.5. (FOUO) 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, but are not thereby necessarily commercial organizations. 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 predominate nature of the organization.

3.6. (FOUO) Communicant means the originator or intended recipient of a communication.

3.7. (FOUO) Communications concerning a U.S. person are those in which the U.S. person is identified in the communication. A U.S. person is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name or manufacturer's name, or the use of a name in a descriptive sense, for example, "Monroe Doctrine," "Boeing 707," is not an identification of a U.S. person.

3.8. ([redacted]) Consent is the agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit collection of information shall be deemed valid consent if given on behalf of such organization by an official or governing body, determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

3.9. (FOUO) Corporation means an organization incorporated in the United States under federal, state, or local law. As regards the corporation's status as a U.S. person, the fact and place of incorporation is determinative. Entirely foreign ownership does not disqualify an organization for treatment as a U.S. person 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.

3.10. (FOUO) 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.

3.11. (FOUO) 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 neutralize such acts. A counterintelligence investigation, for purposes of these procedures, does not include counterespionage operations undertaken against foreign powers.

3.12. (FOUO) 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.

3.13. (FOUO) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among foreign powers or between a foreign power and officials of a foreign power (but not including communications intercepted by electronic surveillance directed at premises used predominantly for residential purposes).

3.14. (FOUO) 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, sabotage, and assassinations for, or on behalf of, foreign powers.

3.15. (FOUO) 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. (Annex A, paragraph 2.2, defines "foreign power" for situations under the Foreign Intelligence Surveillance Act (FISA). Portions of that definition should also be used in certain situations as noted in paragraphs 6.1.b. and 8.1.e.(1).)

[redacted]

3.17. (FOUO) For the purposes of this USSID, the Intelligence Community refers to:

a. The Central Intelligence Agency;

b. The National Security Agency;

c. The Defense Intelligence Agency;

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;

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

h. The intelligence elements of the Department of Treasury and the Department of Energy.

i. The intelligence elements of the Federal Bureau of Investigation (FBI); and

[redacted]

j. The intelligence elements of the Drug Enforcement Administration (DEA).

3.18. (FOUO) Interception means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

3.19. (FOUO) International terrorist activities mean any activity or activities that:

a. Involve killing, causing serious bodily harm, kidnapping or violent destruction of property, or an attempt or credible threat to commit such acts;

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.

3.20. (FOUO) 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. In this context, the criminal law includes federal statutes, federal regulations, and the Uniform Code of Military Justice.

3.21. (FOUO) Law enforcement authorities include military police, local police, state police, the FBI, 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 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.

3.22. (FOUO) 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.

3.23. (FOUO) Personnel security means the protection resulting from measures designed to ensure 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 ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

3.24. (FOUO) 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.

3.25. (FOUO) 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.

3.26. (FOUO) 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.

[redacted]

3.29. (FOUO) Technical data base means information retained for cryptanalytic or traffic analytic purposes.

3.30. (FOUO) United States, when used to describe a place, includes the terrorities of the United States.

3.31. [redacted] U.S. person means a citizen of the United States, an alien lawfully admitted for 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.

a. The term "U.S. person" includes U.S. flag, nongovernmental aircraft or vessels. The term does not include a corporation incorporated in the United States that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

b. For purposes of intentionally collecting the communications of a particular person, the term "U.S. person" also includes any alien known to be presently in the United States, any group of such aliens or American citizens, any corporation, corporate subsidiary, or other legal entity having its principal place of business in the United States, and U.S. flag, nongovernmental aircraft or vessels; provided, however, that it shall not include:

(1) Any alien (other than an alien lawfully admitted for permanent residence) who, on the basis of available, reliable information, is reasonably believed to be an officer, employee, or accredited representative of a foreign power;

(2) Any group of such aliens; or

(3) Any corporation, corporate subsidiary, or other legal entity which on the basis of available, reliable information, is reasonably believed to be owned or controlled, directly or indirectly, by a foreign power.

c. The following guidelines will apply in determining whether a person is a U.S. person:

(1) A person known to be currently in the United States will be treated as a U.S. person unless that person is positively identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. person.

(2) A person known to be currently outside the United States, or whose location is not known, will not be treated as a U.S. person unless such person can be identified positively as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. person.

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

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

3.32. (FOUO) USSS means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the military services authorized to conduct signals intelligence and such other entities (other than the FBI) as are authorized by the National Security Council or the Secretary of Defense to conduct SIGINT.

SECTION 4 - POLICY

4.1. (U) The SIGINT mission of the USSS includes the collection, processing, storage, and dissemination of foreign communications (plaintext and encrypted) passed by radio, wire, or other electromagnetic means. It is the policy of the USSS to target or collect foreign communications. The USSS will not intentionally collect the communications of U.S. persons or communications that refer to U.S. persons except as authorized pursuant to the procedures contained in this USSID or its annexes. The USSS will only process and disseminate communications of U.S. persons, or that refer to U.S. persons, as provided for in this USSID.

SECTION 5 - COLLECTION

5.1. (U) The Director, NSA, will consider requests to collect the communications of U.S. persons, or communications that refer to U.S. persons, only if one of the following criteria is satisfied:

a. The U.S. person has given consent and has executed the consent form as set forth in Annex I. Once the consent form has been executed, the Director, NSA, may authorize the collection. The Director, NSA, shall notify the Attorney General of each consensual collection.

b. The U.S. person is a foreign power or an agent of a foreign power. The purpose of the collection must be the acquisition of foreign intelligence or counterintelligence. It is also necessary that the information be unobtainable by less intrusive techniques. In this case, the Director, NSA, may:

(1) Submit an application for the collection in accordance with the FISA when the U.S. person is in the United States and the communications sought are those of that U.S. person (see Annex A).

(2) Request the Attorney General to authorize collection when the U.S. person is outside the United States, when the U.S. person is in the United States and only communications that refer to that person are sought, or when a U.S. person as defined in Section 3.31.b. is in the United States.

(3) Authorize the collection if an emergency situation exists and the U.S. person is outside the United States.

5.2. (U) In emergency situations, the Director, NSA, may approve for foreign intelligence or counterintelligence purposes the collection of communications of U.S. persons, or communications that refer to U.S. persons, when such persons are outside the United States and when securing the prior approval of the Attorney General is not practical.

a. An emergency situation exists when:

(1) The time required to secure Attorney General 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) Any 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.

b. The Director, NSA, shall notify the DoD General Counsel and the Attorney General as soon as possible of the nature of the collection, the circumstances surrounding its authorization, and the results thereof.

c. Such collection may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

[redacted]

SECTION 6 - PROCESSING

6.1. [redacted] Foreign communications of, or concerning, U.S. persons must be processed in accordance with the following limitations:

[redacted]

[redacted]

6.3. [redacted] Except as approved under this USSID and its annexes, no collection may be directed that brings about the intentional interception and recording of communications solely between U.S. persons. [redacted] Those non-foreign communications that may indicate threat of death or serious bodily harm to any person, or [redacted] reveal a potential vulnerability to United States Communications Security, should be forwarded to NSA/CSS,

[redacted]

SECTION 7 - STORAGE

7.1. (S[redacted] Foreign communications of, or concerning, U.S. persons that are intercepted by the USSS may be retained in their original form or as transcribed:

[redacted]

b. If dissemination of such communications without elimination of references to such U.S. persons would be permitted under Section 8, below.

7.2. (FOUO) Where practicable and when recognizable, information acquired as a part of, or incidental to, authorized collection activities wherein the identification of a U.S. person is not necessary [redacted] for dissemination under Section 8, the U.S. person's identity shall be deleted and replaced by a generic term.

7.3. (FOUO) Storage systems shall be reasonably designed to limit access to information about U.S. persons to those with a need to know.

7.4. (FOUO) Intelligence reports based on foreign communications must be stored in accordance with the Privacy Act. Although Section 8 permits the dissemination of information containing the names of U.S. persons, such names will be deleted prior to permanent storage of intelligence reports in name retrievable files, [redacted]

7.5. (FOUO) Information about U.S. persons other than that covered by this section shall be stored only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

SECTION 8 - DISSEMINATION

8.1. (U) Dissemination of information derived from foreign communications that includes an identification of a U.S. person may be made only if one of the following criteria is met:

a. The U.S. person has consented to the use of communications of, or concerning, him or her and has executed the applicable consent form (see Annex I).

b. The information is available publicly; for example, the information is derived from unclassified collateral information available to the general public.

c. The identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance; for example, the identity of a senior official in the Executive Branch. Such officials, when identified, will be identified only by their official titles; for example, "President of the United States."

d. The communication or information indicates that the U.S. person may be an agent of a foreign power.

e. The communication or information that is being disseminated indicates that the U.S. person may be:

(1) A foreign power as defined in Annex A, 2.2.d. and f.;

(2) Residing outside the United States and holding an official position in the government or military forces of a foreign power such that information about his activities would constitute foreign intelligence;

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

(4) Acting in collaboration with an intelligence or security service of a foreign power, and the U.S. person has, or has had, access to information or material classified by the United States;

f. The communication or information indicates that the U.S. person may be the target of intelligence activities of a foreign power.

g. The communication or information indicates that the U.S. person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified.

h. The communication or information indicates that the U.S. person may be engaging in international terrorist activities.

i. The interception of the U.S. person's communication was authorized by a court order issued pursuant to Section 105 of the FISA and the communication may relate to the foreign intelligence purpose of the surveillance. (See Annex A.)

j. The communication or information is evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes; for example, the communication or information indicates a possible threat to the life or physical safety of any person.

[redacted]

8.5. [redacted] Any proposed report or translation based on, relating to, or relaying the contents of a privileged communication, for example, attorney-client, doctor-patient, involving a U.S. person, including for this purpose, the U.S. Government, must be referred [redacted] for review prior to publication.

8.6. (FOUO) Dissemination other than that described in this section must be approved by the General Counsel to ensure compliance with applicable laws, executive orders, and regulations.

SECTION 9 - RESPONSIBILITIES

9.1. (FOUO) Inspector General - The Inspector General is assigned overall staff responsibility for overseeing NSA/CSS compliance with this USSID. In carrying out this responsibility, the Inspector General:

a. Annually conducts a detailed inspection of NSA/CSS activities to ensure compliance with this USSID.

b. Reports to the Director, NSA, annually (1 October) concerning NSA/CSS compliance with this USSID.

c. Establishes procedures for reporting by Key Component and Field Chiefs of their activities and practices to the Inspector General.

d. Reports quarterly with the Director and General Counsel to the Intelligence Oversight Board through the Inspector General for Defense Intelligence.

9.2. (FOUO) The General Counsel:

a. Actively assists the Inspector General in the annual inspection of NSA/CSS activities, as required.

b. At the request of the Director, Deputy Director, Key Components Chiefs, or the Inspector General, reviews and assesses for legal implications new major requirements levied on the NSA/CSS or internal initiatives that may involve the rights of U.S. persons.

c. Reviews and obtains from the Attorney General necessary approval of new procedures.

d. Advises the Director and senior staff, NSA/CSS, of new legislation and/or case laws that may impact on NSA/CSS missions, functions, operations, activities, and practices.

e. Reports, as required, to the Intelligence Oversight Board and provides copies of such reports to the Director and affected agency elements.

9.4. (FOUO) All Elements of the USSS:

a. Implement this directive upon receipt. Ensure adherence to the provisions of this USSID and appropriate annexes in the conduct of SIGINT operations.

b. Amend and supplement existing formal publications and informal operating instructions to conform with this USSID.

c. Prepare new procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: [redacted]

d. Immediately inform the DDO of any tasking received that appears to require actions at variance with this USSID.

SECTION 10 - ACCOUNTABILITY

[redacted]

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

20 October 1980

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE (USSID)

18

ANNEX A

PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)

LETTER OF PROMULGATION

(U) This annex is issued separately for use by elements of the USSS only when conducting electronic surveillance pursuant to the Foreign Intelligence Surveillance Act (FISA). Such surveillance will be conducted only upon notification by NSA/CSS.

B. R. INMAN
Vice Admiral, U.S. Navy
Director, NSA/Chief, CSS

[redacted]

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 20 OCTOBER 2010

SECURITY CLASSIFICATION

CHANGE REGISTER

CHANGE			ENTERED	
NO.	DATE	AUTHORITY *(Msg Cite/DTG, Hard Copy (HC), OPSCOMM)*	DATE	BY

FORM A7093 REV AUG 76 *(Supersedes A7093 Nov 72 which is obsolete)*

SECURITY CLASSIFICATION

USSID 18
20 October 1980

ANNEX A

PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)
INTELLIGENCE SURVEILLANCE ACT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) The Foreign Intelligence Surveillance Act (FISA) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. These electronic surveillance activities involve either the acquisition of wire communications by direct access in the United States, the acquisition of radio communications where all parties to that communication are located in the United States, the intentional collection of the communications of a particular, known U.S. person who is in the United States, or the acquisition of information within the United States from other than wire or radio communications.

1.2. (U) These procedures apply to the collection, processing, storage, and dissemination of communications collected by electronic surveillance authorized pursuant to FISA, Public Law 95-511 ("the Act"). The procedures also apply to the acquisition of technical intelligence, other than the spoken communications of individuals, conducted under certification of the Attorney General, pursuant to Section 102(a)(1)(A)(ii) of the Act.

SECTION 2 - DEFINITIONS

2.1. (U) In addition to the definitions in Section 3 of USSID 18, the following definitions shall apply to this annex. If a term is defined in Section 3 of USSID 18 and in this annex, only the definition in this annex shall be used for surveillance activities conducted pursuant to the Act.

2.2. (U) "Foreign power" means -

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

b. A faction of a foreign nation, or nations, not substantially composed of U.S. persons;

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

d. A group engaged in international terrorism or activities in preparation therefor;

e. A foreign-based political organization, not substantially composed of U.S. persons; or

f. An entity that is directed and controlled by a foreign government or governments.

2.3. (U) "Foreign intelligence information" means -

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

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

(2) Sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(3) Clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

b. Information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to -

(1) The national defense or the security of the United States; or

(2) The conduct of the foreign affairs of the United States.

2.4. (U) "Contents," when used with respect to a communication, include any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

2.5. (U) "Electronic surveillance" means -

a. The acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by, or intended to be received by, a particular, known U.S. person who is in the United States,

if the contents are acquired by intentionally targeting that U.S. person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

b. 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;

c. 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

d. 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.

NOTE: Communication intercept activity 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 meaning of this definition.

2.6. (U) "U.S. person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in Section 101(a)(20) 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, as defined in subsections 2.2a, b, or c.

2.7. (U) "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.

SECTION 3 - GENERAL

3.1. (U) Collection of foreign intelligence information by electronic surveillance as defined in paragraph 2.5 shall be accomplished only in accordance with an order of the United States Foreign Intelligence Surveillance Court (USFISC) or a certification of the Attorney General. In any case in which it is necessary for the USSS to conduct electronic surveillance, a request to secure a court order or Attorney General certification will be forwarded by the appropriate Key Component through the General Counsel to the Director. Only targets that meet the definition of either agent of a foreign power or foreign power may be considered for approval pursuant to the Act.

SECTION 4 - MINIMIZATION PROCEDURES

4.1. (U) Each surveillance authorized pursuant to the Act must be conducted pursuant to the minimization procedures approved by the USFISC or the Attorney General for that particular surveillance. Minimization procedures will be attached to each court order or Attorney General certification that is issued and will regulate the collection, processing, storage, and dissemination of information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

4.2. (U) The Attorney General has approved standard minimization procedures applicable to electronic surveillance activities pursuant to the Act. These minimization procedures apply to electronic surveillances authorized by the USFISC or the Attorney General pursuant to the Act, except as provided in subsection 4.4 of this annex.

MINIMIZATION PROCEDURES

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978, the following procedures have been adopted by the Attorney General, and shall be followed by the National Security Agency in implementing this electronic surveillance as ordered by the Court: (U)

Sec. 1 - Applicability and Scope.

[redacted]

Sec. 2. Definitions.

In addition to the definitions in Section 2 of this annex, the following definitions shall apply to these procedures:

(a) Acquisition means the interception by the National Security Agency through electronic means of a communication to which it is not an intended party and the processing of the contents of that communication into an intelligible form intended for human inspection. (U)

(b) Available publicly means information that a member of the public could obtain on request, by research in public sources, or that has been obtained by casual observation. (U)

(c) Consent is the agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit collection of information shall be deemed valid consent if given on behalf of such organization by an official or governing body, determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

(d) Identification of a United States person means the name, unique title, address or other personal identifier of a U.S. person in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense; for example, "Monroe Doctrine," is not an identification of a U.S. person. (U)

(e) Technical data base means information retained for cryptanalytic or traffic analytic purposes.

(f) U.S. person. The following guidelines will apply in determining whether a person is a U.S. person:

(1) A person known to be currently in the United States will be treated as a U.S. person unless that person is positively identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. person.

(2) A person known to be currently outside the United States, or whose location is not known, will not be treated as a U.S. person unless such person can be identified positively as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. person.

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

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

Sec. 3. Acquisition.

The collection of information by electronic surveillance subject to these procedures shall be accomplished in accordance with the certification of the Attorney General or the court order authorizing such surveillance and will be conducted by technical means, and in a manner designed to minimize to the greatest extent reasonably feasible the acquisition of information which is not relevant to the authorized purpose of the surveillance. Collection personnel will monitor the collection of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications of U.S. persons outside the authorized scope of the surveillance or information concerning U.S. persons not related to the purpose of the surveillance. Personnel who process intercepted data into an intelligible form intended for inspection by analysts will discard inadvertently acquired communications of, or information concerning, U.S. persons at the earliest practicable point in the processing cycle at which such communication or information can be identified as clearly not relevant to the authorized purpose of the surveillance. Communications of, or information concerning, U.S. persons which may be related to the purpose of the surveillance may be forwarded to analytic personnel who are responsible for producing intelligence information from the collected data. Any such communication or information acquired in the course of an authorized surveillance may be retained and disseminated only in accordance with Sections 4 and 5 of these procedures. (S)

[redacted]

[redacted]

Sec. 5. Dissemination.

(a) Dissemination of intelligence reports or translations that include an identification of a U.S. person may be made only if one of the following criteria is met:

The U.S. person has consented to the use of communications of, or concerning, him or her and has executed the applicable consent form (see Annex I).

The information is available publicly; for example, the information is derived from unclassified collateral information available to the general public.

The identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance; for example, the identity of a senior official

in the Executive Branch. Such officials, when identified, will be identified only by their official titles; for example, "President of the United States."

The communication or information indicates that the U.S. person may be an agent of a foreign power.

The communication or information that is being disseminated indicates that the U.S. person may be:

A foreign power as defined in this annex, paragraph 2.2d and f;

Residing outside the United States and holding an official position in the government or military forces of a foreign power such that information about his activities would constitute foreign intelligence;

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

Acting in collaboration with an intelligence or security service of a foreign power, and the U.S. person has, or has had, access to information or material classified by the United States;

The communication or information indicates that the U.S. person may be the target of intelligence activities of a foreign power.

The communication or information indicates that the U.S. person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified.

The communication or information indicates that the U.S. person may be engaging in international terrorist activities.

The interception of the U.S. person's communication was authorized by a court order issued pursuant to Section 105 of the Act and the communication may relate to the foreign intelligence purpose of the surveillance.

The communication or information is evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes;

for example, the communication or information indicates a possible threat to the life or physical safety of any person.

(b) A report based on a communication of, or information concerning, an unconsenting U.S. person that is not publicly available may be disseminated without regard to the limitations in (a) above if the identity of the U.S. person is deleted and a generic term or symbol is substituted so that the information in the context of the communication cannot reasonably be connected with an identifiable U.S. person. (U)

(c) Reports based on the communications of, or containing information concerning, an identified unconsenting U.S. person may only be disseminated to a recipient requiring the identity of such person in the performance of official duties. (U)

(d) Upon recognition that a radio communication to which all parties are in the United States has been unintentionally acquired under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, such communication shall be destroyed promptly unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person. (U)

4.3. (C) If, during the course of electronic surveillance authorized by Attorney General certification, the contents of any communication to which a U.S. person is a party are acquired, that communication shall not be disclosed, disseminated, or used for any purpose or retained for longer than 24 hours after recognition unless a court order is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

4.4. (C) While the minimization procedures set forth in 4.2 and 4.3 are the standard procedures used for surveillance activities conducted by NSA pursuant to the Act, it may be necessary to develop special procedures on a case-by-case basis. Those procedures will be provided directly to the personnel responsible for collecting, processing, storing, and disseminating the information collected by that particular electronic surveillance.

SECTION 5 - RESPONSIBILITIES

[redacted]

5.2. (U) The General Counsel will review requests to conduct electronic surveillance pursuant to the Act and will prepare applications for securing court orders and requests for Attorney General certifications.

ANNEX B

OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U)

SECTION 1 - GENERAL

1.1. (U) In accordance with the provisions of Section 2-309(c) of E.O. 12036, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the Bureau in the conduct of its lawful functions. When requesting such assistance, the FBI shall certify to the General Counsel of NSA that such equipment or technical knowledge is necessary to the accomplishment of one or more of the Bureau's lawful functions.

1.2. (U) NSA may also provide expert personnel to assist Bureau personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence or counterintelligence. When requesting the assistance of expert personnel, the FBI shall certify to the General Counsel that such assistance is necessary to collect foreign intelligence or counterintelligence and that the approval of the Attorney General (and, when necessary, a warrant from a court of competent jurisdiction) has been obtained.

SECTION 2 - CONTROL

2.1 (U) No operational assistance as discussed in Section 1 shall be provided without the express permission of the Director, NSA/Chief, CSS.

USSID 18
20 October 1980

ANNEX C

SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U)

SECTION 1 - POLICY

1.1. (C) Signals intelligence support to U.S. and Allied military exercise command authorities is provided for in USSID 56 and DoD Directive 5200.17 (M-2). JCS Secretary's Memorandum 485-73, annexed to USSID 4, establishes doctrine and procedures for providing signals intelligence support to military commanders. The procedures in this annex provide policy guidelines for safeguarding the rights of U.S. persons in the conduct of Exercise SIGINT support activities.

SECTION 2 - DEFINITIONS

2.1. (U) Military Tactical Communications mean United States and Allied military exercise communications, within the United States and abroad, that are necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

SECTION 3 - PROCEDURES

3.1. (C) The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S. persons.

a. Collection efforts will be conducted in such a manner as to avoid, to the extent feasible, the intercept of non-exercise-related communications.

b. Military tactical communications may be stored and processed without deletion of references to U.S. persons if the names and communications of the U.S. persons who are exercise participants, whether military, government, or contractor, are contained in, or such communications constitute, exercise-related communications or fictitious communications or information prepared for the exercise.

c. Communications of U.S. persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible [redacted]

d. Dissemination of military exercise communications, exercise reports, or information files derived from such communications shall be limited to those authoritiies and persons participating in, or conducting, reviews and critiques thereof.

USSID 18
20 October 1980

ANNEX D

TEST AND EVALUATION OF ELECTRONIC EQUIPMENT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) This annex applies to the testing (including calibration) and evaluation of electronic equipment that has the capability to intercept communications. Testing and evaluations of such electronic equipment will be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons.

SECTION 2 - PROCEDURES

2.1. (U) The USSS may test electronic equipment that has the capability to intercept communications subject to the following limitations:

a. To the maximum extent that is practical, the following should be used —

(1) Laboratory-generated signals;

(2) Department of Defense official agency communications with consent from an appropriate DoD official;

(3) Official government agency communications with consent from an appropriate official of the originating agency;

(4) Individual government employee communications with consent from the employee; or

(5) Communications transmitted between terminals located outside the United States not used by any known U.S. person.

b. Where it is not practical to test electronic equipment solely against signals described in paragraph 2.1a, above, testing may be conducted, provided —

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

(2) No particular U.S. person is targeted intentionally without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and

(3) The test does not exceed 90 calendar days.

c. Where the test involves communications other than those identified in 2.1a and a test period longer than 90 days is required, a test proposal and plan shall be submitted to the Attorney General for approval. Such proposals and plans shall be submitted to the Director, NSA, through the General Counsel, NSA, for transmission to the Attorney General. 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.

2.2. (U) The content of any communication acquired during a test and evaluation shall be:

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

b. Disclosed only to persons conducting or evaluating the test; and

c. Destroyed upon completion of the testing.

2.3. (U) 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, evaluation, or collection-avoidance purposes. No content of any communication may be retained or used.

USSID 18
20 October 1980

ANNEX E

COMMUNICATIONS SECURITY (U)

SECTION 1 - PURPOSE

1.1. (U) This annex is provided for information purposes only since USSID are not directive for Communications Security (COMSEC) operations. Implementation of COMSEC surveillance policy and procedures is in National COMSEC Instruction (NACSI) 4000.

SECTION 2 - DEFINITIONS

2.1. (U) Communications security is the protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to the national security and to ensure the authenticity of such telecommunications. Communications security also includes the protection of communications containing government-derived unclassified information that relates to the national security. It includes the protection of telecommunications of organizations holding classified Defense contracts or otherwise involved in the industrial security program. It also includes the assessment of the vulnerability of United States communications to foreign electronic surveillance.

2.2. (U) 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, NSA, acting for the Secretary in executing responsibilities as executive agent, that carries out any of the communications security activities of the United States Government.

2.3. (U) 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 reception over time.

SECTION 3 - PROCEDURES

3.1. (U) Communications security monitoring may be directed against the communications of U.S. persons only:

a. With the consent of one of the parties to the communication;

b. As a part of a communication vulnerability survey (see paragraph 3.2); or

c. As part of a hearability survey.

3.2. (U) NSA may survey or authorize the survey by other communications security entities of the transmission facilities of communications common carriers, other private commercial entities, or the federal government to determine the potential vulnerability of those facilities to surveillance activities conducted by foreign powers.

a. No communication vulnerability survey may be conducted without the prior written approval of the Deputy Director for Communications Security, NSA.

b. Information collected during a communications vulnerability survey must be stored and processed as follows:

(1) No transmission may be acquired aurally.

(2) No transmission may be demultiplexed or demodulated for any purpose except to detect by a visual display device a test tone placed on the transmission by the owner or operator of the facility.

(3) No content may be acquired and no transmission may be recorded.

(4) Reports and logs may be compiled and retained, provided that no report or log may identify any person or entity except to the extent of identifying those 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, and their identities are relevant to the national security in light of the vulnerability of the facilities, the identity of such users may be obtained, provided such identities may not be obtained from the content of the transmissions themselves. The reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

3.3. (U) NSA may conduct, or may authorize the conduct of, hearability surveys of telecommunications that are transmitted in the United States.

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

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

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

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

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

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

USSID 18
20 October 1980

ANNEX F

SEARCH AND DEVELOPMENT OPERATIONS (U)

SECTION 1 - GENERAL

1.1. (C) This annex provides the procedures for safeguarding the rights of U.S. persons when conducting SIGINT search and development activities.

[redacted]

b. Communications originated or intended for receipt in the United States or originated or intended for receipt by U.S. persons shall be processed in accordance with Section 6 of USSID 18. [redacted]

c. Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify U.S. persons, provided that communications equipment nomenclature may be disseminated. Information that reveals a vulnerability to United States communications security may be disseminated to the appropriate communications security authorities.

d. All information obtained in the process of search and development that appears to be of foreign intelligence value may be forwarded to the proper analytic office within NSA for processing and dissemination in accordance with relevant portions of USSID 18.

SECTION 2 - CONTROL

2.1. (U) The DDO shall ensure compliance with these procedures.

ANNEX H

TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SIGINT COLLECTION EQUIPMENT (U)

SECTION 1 - APPLICABILITY

1.1. (U) This annex applies to the training of personnel by USSS components in the operation and use of SIGINT collection equipment. This annex does not apply to the interception of communications with the consent of one of the parties to the communication.

SECTION 2 - DEFINITION

2.1. (U) 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.

SECTION 3 - POLICY

3.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment is conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons who have not given consent.

SECTION 4 - PROCEDURES

4.1. (U) The training of USSS personnel in the operation and use of SIGINT collection equipment shall include guidance concerning the requirements and restrictions of the FISA, Executive Order 12036, and USSID 18 with respect to the unauthorized acquisition, storage, and dissemination of the content of communications of U.S.persons.

4.2. (U) The use of SIGINT collection equipment for training purposes is subject to the following limitations:

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

b. The contents of private communications of nonconsenting U.S. persons may not be acquired aurally unless the person is an authorized target of electronic surveillance; and

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

4.3. (U) The limitations in paragraph 4.2 do not apply in the following instances:

a. 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.

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

4.4. (U) Information collected during training that involves authorized intelligence targets may be stored in accordance with Section 7 of USSID 18 and disseminated in accordance with Section 8 of USSID 18. Information other than distress signals 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 outside the USSS for any purpose. Distress signals should be referred to the DDO.

ANNEX I

SAMPLE CONSENT FORMS (U)

SECTION 1 - PURPOSE

1.1. (U) The consent forms, shown herein, are samples of those used to record an agreement betweeen the U.S. person and NSA concerning the collection and dissemination of foreign communications by or about the U.S. person.

1.2. (U) The first sample form is for consent to collect and disseminate a U.S. person's communications and references to that person in foreign communications. The second sample form is for consent to collect and disseminate only references to the U.S. person in foreign communications.

USSID 18, ANNEX I
20 October 1980

EXECUTIVE ORDER

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____(full name)_____, _____(title)_____, hereby consent to the National Security Agency undertaking to seek and disseminate communications to or from or referencing me in foreign communications for the purpose of _____.

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12036 procedures, this consent covers only information that relates to the purpose stated above and is effective for the period ____(date)____ to ____(date)____.

Signals intelligence reports containing information derived from communications to or from me may only be disseminated to me and to _____. Signals intelligence reports containing information derived from communications referencing me may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12036.

(SIGNATURE)

(TITLE) (DATE)

SAMPLE

USSID 18, ANNEX I
20 October 1980

EXECUTIVE ORDER

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____(full name)_____, _____(title)_____, hereby consent to the National Security Agency undertaking to seek and disseminate references to me in foreign communications for the purpose of _____.

This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12036 procedures, this consent covers only references to me in foreign communications and information derived therefrom that relate to the purpose stated above. This consent is effective for the period _____(date)_____ to _____(date)_____.

Signals intelligence reports containing information derived from communications referencing me and related to the purpose stated above may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12036.

(SIGNATURE)

(TITLE) (DATE)

SAMPLE