

~~SECRET//COMINT//X1~~



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
NSA/CSS POLICY 1-23



Issue Date: 11 March 2004  
Revised:

---

**(U) PROCEDURES GOVERNING NSA/CSS ACTIVITIES  
THAT AFFECT U.S. PERSONS**

**(U) PURPOSE AND SCOPE**

(U) This Policy is issued to comply with DoD Directive 5240.1 (Reference a), which implements Public Law 95-511 (the Foreign Intelligence Surveillance Act of 1978, as amended; Reference b), Part 2 of Executive Order (E.O.) 12333 (Reference c), and E.O. 12863 (Reference d). It establishes procedures and assigns responsibilities to ensure that the signals intelligence (*SIGINT*) and information assurance (IA) missions of the National Security Agency/Central Security Service (NSA/CSS) are conducted in a manner consistent with the privacy rights of *U.S. persons* and as required by law, executive orders, Department of Defense (DoD) policies and instructions, and internal NSA/CSS policy.

(U) This Policy applies to all NSA/CSS elements.

MICHAEL V. HAYDEN  
Lieutenant General, USAF  
Director, NSA/Chief, CSS

Endorsed by  
Director of Policy

Encl:

(U) Annex – Classified Annex to DoD Procedures under Executive Order 12333

DISTRIBUTION III  
PLUS: OGC (25 Stock Copies)  
DC31  
DC324 (VR)

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

(U) This Policy 1-23 supersedes Directive 10-30, dated 20 September 1990, and Change One thereto, dated June 1998.

(U) OPI: OGC (963-3121s)

(U) The compilation of the information contained in this document should be treated as SECRET//COMINT due to the classification of the Annex; upon removal of the Annex, this document may be downgraded to CONFIDENTIAL. No section of this document shall be released without approval from the Office of Policy and Records, DC3.

### (U) POLICY

1. (U) NSA/CSS shall collect, process, retain, and disseminate information about U.S. persons only as prescribed in DoD Directive 5240.1 (Reference a), DoD Regulation 5240.1-R (Reference e) and the Classified Annex to DoD Procedures under Executive Order 12333 (hereafter referred to as the Classified Annex; Reference f).

### (U) PROCEDURES

2. (U) Signals Intelligence. The signals intelligence (SIGINT) mission of the NSA/CSS is to collect, process, retain, and disseminate signals intelligence information for national foreign intelligence (and counterintelligence) purposes and in support of U.S. military operations. NSA/CSS shall intentionally collect only foreign communications. NSA/CSS shall not intentionally collect U.S. person communications. The Director, NSA/Chief, CSS may authorize exceptions only pursuant to the procedures contained in DoD Regulation 5240.1-R (Reference e) and the Classified Annex thereto (Reference f).

a. (U) Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, as amended (Reference b), requires a court order issued by a judge appointed pursuant to the Act or a certification of the Attorney General of the United States issued pursuant to Section 102(a) of the Act. The Director, NSA/Chief, CSS or Deputy Director, NSA must approve applications for a court order, which must be submitted through the DoD General Counsel to the Attorney General. The Director, NSA/Chief, CSS or Deputy Director, NSA may submit requests for Section 102(a) certifications directly to the Attorney General. The Director, NSA/Chief, CSS or Deputy Director, NSA may contact the Attorney General in an emergency and the Attorney General may approve the surveillance pending subsequent court proceedings.

b. (U) Electronic surveillance, as defined in Appendix A to DoD Regulation 5240.1-R (Reference e), directed against U.S. persons who are outside the U.S. requires approval of the Attorney General. The Director, NSA/Chief, CSS or the Deputy Director may request approval of such surveillances by forwarding a request to the Attorney General. In emergency situations, as described in Procedure 5, Part 2.D., of Reference e, the Director, NSA/Chief, CSS, Deputy Director, NSA or the Signals Intelligence Director, NSA, may authorize electronic surveillance, for no more than 72 hours,

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

of U.S. persons who are outside the U.S. Such authorization is subject to the limitations of Procedure 5, Part 2.D. The DoD General Counsel shall be notified promptly of any such surveillance.

3. (U) Information Assurance. The information assurance (IA) mission assigned to NSA/CSS by National Security Directive (NSD) 42 (Reference g), Executive Order 12333 (Reference c), and other applicable law and policy direction includes the responsibility to examine national security systems, as that term is defined by 40 U.S.C. § 1452 (Reference h) and other applicable law, and evaluate their vulnerability to foreign interception and exploitation. In a manner consistent with the provisions of the Computer Security Act of 1987 (Reference i) and implementing procedures agreed to by NSA/CSS and the National Institute of Standards and Technology, the Agency is also authorized to provide IA support for non-national security systems. Any IA activities undertaken by the Agency, including those involving monitoring of official communications, shall be conducted in strict compliance with law, Executive Order and implementing procedures, and applicable Presidential directive. Any monitoring undertaken for communications security purposes ("COMSEC monitoring") shall be conducted in accordance with the provisions of National Telecommunications and Information Systems Security Directive (NTISSD) No. 600 (Reference j) or other special procedures approved by the Attorney General. In addition to the responsibility to conduct COMSEC monitoring and to examine national security systems for vulnerabilities to foreign exploitation, NSD 42 (Reference g) also requires NSA/CSS to disseminate information on threats to national security systems, regardless of the source of the threat. Title II of the Homeland Security Act of 2002 (Reference k) imposes similar requirements with respect to the protection of the United States' critical infrastructure. The Information Assurance Director is hereby designated to act for Director, NSA/Chief, CSS in the issuance of written approval to conduct the information assurance activities assigned to the Agency, to include the conduct of activities that may result in the collection of US person information as defined in DoD Regulation 5240.1-R (Reference e) and other applicable guidance.

#### (U) RESPONSIBILITIES

4. (U) The NSA General Counsel (GC) and Inspector General (IG) shall:

a. (U) Conduct appropriate oversight to prevent or detect violations of E.O. 12333, DoD Directive 5240.1 (References c and a), this Policy, and any directives and regulations issued thereunder.

b. (U) Forward to the Intelligence Oversight Board (IOB) of the President's Foreign Intelligence Advisory Board (PFIAB), through the Assistant to the Secretary of Defense (Intelligence Oversight (ATSD (IO))), reports of activities that they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive, and provide other reports or information that the IOB or ATSD (IO) requires.

~~SECRET//COMINT//X1~~

(b) (1)  
(b) (3) - 50 USC 403

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

5. (U) The NSA Inspector General shall:

a. (U) Conduct regular inspections of NSA/CSS activities for compliance with the law, executive orders, and related directives.

(S)

b. (U//FOUO) Perform general oversight of the SIGINT activities of the [redacted] [redacted] for compliance with Executive Order 12333 (Reference c) and related laws and directives.

c. (U) Establish reporting procedures to be followed by the Directors, Associate Directors and Principal Directors, Chiefs of NSA/CSS Field Activities, and NSA/CSS Representatives regarding their activities and practices.

d. (U) Consult with the NSA General Counsel on matters involving interpretation or possible violations of law, executive orders, or directives.

e. (U) Submit, semiannually, a comprehensive report to the Director and Deputy Director on the results of the IG's oversight activities.

f. (U) Report, as required by E.O. 12333 and 12863 (References c and d) and other authorities, to the ATSD (IO) and the IOB.

6. (U) The NSA General Counsel shall:

a. (U) Provide legal advice and assistance to all NSA/CSS elements regarding the activities covered by this Policy.

b. (U) Assist NSA/CSS activities as requested in developing such guidelines and working aids as are necessary to ensure compliance with this Policy.

c. (U) Assist the NSA Inspector General in inspections and oversight of NSA/CSS activities, as required.

d. (U) Review and assess for legal implications, as requested by the Director NSA/Chief CSS, Deputy Director NSA, SIGINT Director, IA Director, Associate Directors, Principal Directors, or the Inspector General, all new major requirements and internally generated NSA/CSS activities.

e. (U) Advise the Director NSA/Chief CSS, Deputy Director NSA, SIGINT Director, IA Director, Inspector General, Principal Directors, and Associate Directors of new legislation and case law which may have an impact on NSA/CSS missions, functions, operations, activities, or practices.

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

- f. (U) Prepare and forward through DoD to the Attorney General any proposed changes to existing procedures or new procedures required by E.O. 12333 (Reference c) or Public Law 95-511 (Reference b).
- g. (U) Report as required by E.O. 12333 and 12863 (References c and d) to the IOB and provide copies of such reports to the Director and affected NSA/CSS elements.
- h. (U) Prepare and process applications for court orders or certifications for electronic surveillance pursuant to the Foreign Intelligence Surveillance Act (Reference b) in accordance with Procedure 5, Part 1, of DoD Regulation 5240.1-R (Reference e).
- i. (U) Prepare and process requests to the Attorney General for electronic surveillance of unconsenting U.S. persons who are outside the U.S. in accordance with Procedure 5, Part 2 of DoD Regulation 5240.1-R (Reference e).
- j. (U) Process requests from any DoD intelligence component, including NSA/CSS, for authority to use signals as described in Procedure 5, Part 5, of DoD Regulation 5240.1-R (Reference e), for periods in excess of 90 days in the development, test, or calibration of electronic equipment that can intercept communications and other electronic surveillance equipment. Forward processed requests to the Attorney General for approval when required.
7. (U) The SIGINT Director, IA Director, Associate Directors, the NSA/CSS Chief of Staff, Principal Directors and Chiefs of NSA/CSS Field Activities shall:
- a. (U) Appoint an intelligence oversight coordinator or senior level official to oversee intelligence oversight within each major element.
- b. (U) Provide training to all *employees* (including contractors and integrees) in order to maintain a high degree of sensitivity to, and understanding of, the laws and authorities referenced in this Policy. Such training shall include both core and advanced intelligence oversight training and refresher training with appropriate testing. All employees shall receive core training, and those with exposure to U.S. person information shall receive appropriate advanced training. Training shall be required at least annually (or more often commensurate with the level of exposure to U.S. person information by the employee). Newly hired employees and reassignees, including contractor personnel and integrees, must be trained upon assignment. Managers shall keep records of training for all employees. The training must cover: E.O. 12333 (Reference c); Procedures 1-4, 14 and 15 of DoD Regulation 5240.1-R (Reference e); other Procedures of the Regulation that apply to the assigned mission; and this policy. Employees involved in the SIGINT process must be familiar with U.S. SIGINT Directive 18 (USSID 18) (Reference l), and employees involved in COMSEC monitoring must be familiar with NTISSD 600 (Reference j).

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

c. (U) Apply the provisions of this Policy to all activities under their cognizance and ensure that all publications (U.S. SIGINT Directives, National COMSEC Instructions, NSA/CSS Management and Administrative Publications, etc.) and instructions for which they are responsible are in compliance with this Policy.

d. (U) Conduct a periodic review of the activities and practices conducted in or under the cognizance of their respective organizations to ensure consistency with the laws and authorities listed in the References section of this Policy.

e. (U) Ensure that all new major requirements levied on NSA and the U.S. Cryptologic System or internally generated NSA/CSS activities are considered for review and approval by the General Counsel. All activities that may raise a question of law or regulation must be reviewed by the General Counsel prior to acceptance or execution.

f. (U) Ensure that necessary special security clearances and access authorizations are provided to the General Counsel and Inspector General to enable them to meet their assigned responsibilities.

g. (U) Report as required and otherwise assist the Inspector General and General Counsel in carrying out their responsibilities to include providing input to the Inspector General for preparation of the joint Inspector General/General Counsel/Director, NSA/CSS quarterly report to the Assistant to the Secretary of Defense (Intelligence Oversight) and the IOB.

h. (U) Develop, in coordination with the General Counsel and Inspector General as required, such specific guidelines and working aids as are necessary to ensure compliance with this Policy. Such guidelines and working aids should be available to employees at all times and must be reviewed by management with employees at least annually.

#### (U) REFERENCES

##### 8. (U) References:

a. (U) DoD Directive 5240.1, DoD Intelligence Activities, dated: 25 April 1988. [http://netinfo.si.nsa/ExternalNSA/www.dtic.mil/whs/directives/cores/pdf/d52401\\_042588/d52401p.pdf](http://netinfo.si.nsa/ExternalNSA/www.dtic.mil/whs/directives/cores/pdf/d52401_042588/d52401p.pdf)

b. (U) Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511 as amended, 50 U.S.C. 1801 et seq. <http://www.n.nsa/GC/practgrps/ops/ops.html>

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

- c. (U) Executive Order 12333, United States Intelligence Activities, dated: 4 December 1981. <http://www.n.nsa/IG/eo1233.html>
- d. (U) Executive Order 12863, President's Foreign Intelligence Advisory Board, dated: 13 September 1993.
- e. (U) DoD Regulation 5240. 1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, dated: 7 December 1982. <http://www.n.nsa/IG/5240.html>
- f. (U) Classified Annex to Department of Defense Procedures Under Executive Order 12333.
- g. (U) National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated: 5 July 1990.
- h. (U) Information Technology Reform Act of 1996, Division E of Public Law 104-106, as codified at 40 U.S.C. 1401 et seq.
- i. (U) Computer Security Act of 1987.
- j. (U) National Telecommunications and Information Systems Security Directive No. 600, Communications Security (COMSEC) Monitoring, dated: 10 April 1990.
- k. (U) Title II of the Homeland Security Act of 2002, Public Law 107-296.
- l. (U) United States Signals Intelligence Directive (USSID) 18, dated: 27 July 1993.
- m. (U) National Security Council Intelligence Directive (NSCID) No. 6, dated: 17 February 1972.

**(U) DEFINITIONS**

9. (U) SIGINT - SIGINT comprises communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, either individually or in combination. Communications intelligence (COMINT) is defined as "technical and intelligence information derived from foreign communications by other than the intended recipients . . ." and " . . . the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means." NSCID 6 (Reference m), Sec. 4(b). Electronics intelligence (ELINT) consists of foreign electromagnetic radiations such as emissions from a radar system. Foreign instrumentation signals intelligence (FISINT) includes signals from telemetry, beaconry, etc.

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Policy 1-23

Dated: 11 March 2004

10. ~~(E)~~ U.S. Person -
- a. (U) A citizen of the United States;
  - b. (U) An alien lawfully admitted for permanent residence in the United States;
  - c. (U) Unincorporated groups and associations a substantial number of the members of which constitute a or b above, or
  - d. (U) Corporations incorporated in the United States, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them. USSID 18 (Reference 1), Section 9.18.

~~(E)~~ The following additional definition applies to the Classified Annex (Reference f). For purposes of intentionally collecting the communications of a particular person, the term "United States person," in addition to the meanings outlined above, includes any alien known to be presently in the United States; any unincorporated association of such aliens or American citizens; the United States operations, office, branch, or representative of a corporation incorporated abroad; any corporation or corporate subsidiary incorporated in the United States; and any U.S. flag non-governmental aircraft or vessel. Provided however, that the term "U.S. person" shall not include

or (ii) a foreign power or powers as defined in Section 101 (a)(1)-(3) of FISA. Classified Annex (Reference f), Section 2.

11. (U) Employee - A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency. DoD Regulation 5240.1-R (Reference e), Appendix A, Definitions.

(b) (1)  
 (b) (3)-50 USC 403  
 (b) (3)-P.L. 86-36

~~SECRET//COMINT//X1~~



~~SECRET//COMINT//X1~~

(b) (1)  
(b) (3)-50 USC 403

(U) ANNEX

(U) CLASSIFIED ANNEX TO DEPARTMENT OF DEFENSE  
PROCEDURES UNDER EXECUTIVE ORDER 12333

Sec. 1: Applicability and Scope (U)

(S//SI) These procedures implement sections 2.3, 2.4, and 2.6 (c) of Executive Order 12333 and supplement Procedure 5 of DoD Regulation 5240.1-R, previously approved by the Secretary of Defense and the Attorney General. They govern the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection, retention and dissemination of communications originated or intended for receipt in the United States, and signals intelligence activities that are directed intentionally against the communications of a United States person who is outside the United States. These procedures also govern the collection, retention and dissemination of information concerning United States persons that is collected by the United States Signals Intelligence System including such activities undertaken by the [redacted] These procedures do not apply to signals intelligence activities that are not required under Executive Order 12333 to be conducted pursuant to procedures approved by the Attorney General. [redacted]

[redacted] Except for matters expressly authorized herein, the limitations contained in Department of Defense Regulation 5240.1-R also apply to the United States Signals Intelligence System. Reference should be made to those procedures with respect to matters of applicability and scope, definitions, policy and operational procedures not covered herein.

Sec. 2: Definitions (U)

(U) The following additional definitions or supplements to definitions in DoD Regulation 5240.1-R apply solely to this Classified Annex:

(S//SI) Agent of a Foreign Power. For purposes of signals intelligence activities which are not regulated by the Foreign Intelligence Surveillance Act (FISA), the term "agent of a foreign power" means:

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

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

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

(c) a person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power 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;

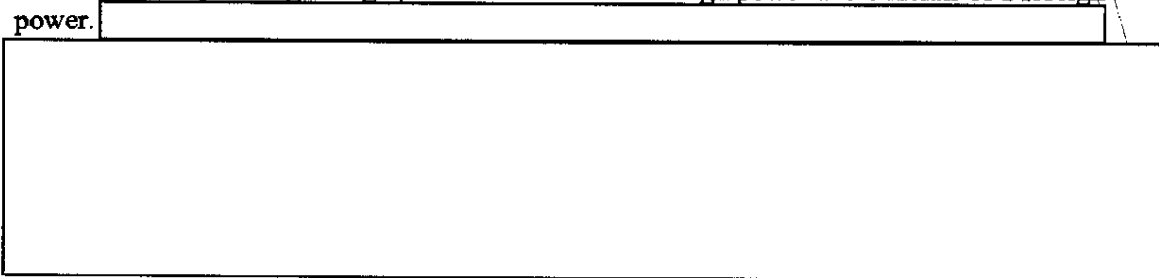
(d) a person in contact with or acting in collaboration with an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has or has had access; or

(e) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power.

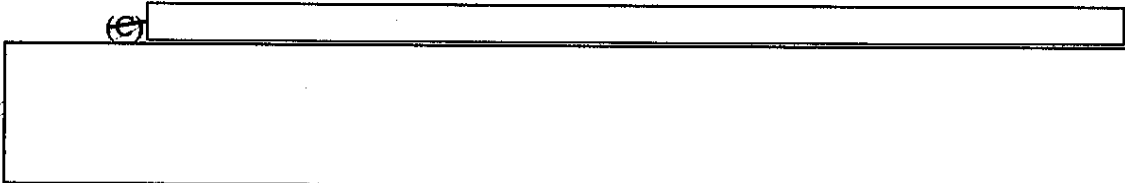
(U) Communicant. The term "communicant" means a sender or intended recipient of a communication.

(U) Consent. For the purposes of signals intelligence activities, 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.

~~(S//SI)~~ Foreign Communication. The term "foreign communication" means a communication that involves a sender or an intended recipient who is outside the United States or that is entirely among foreign powers or between a foreign power and officials of a foreign power.



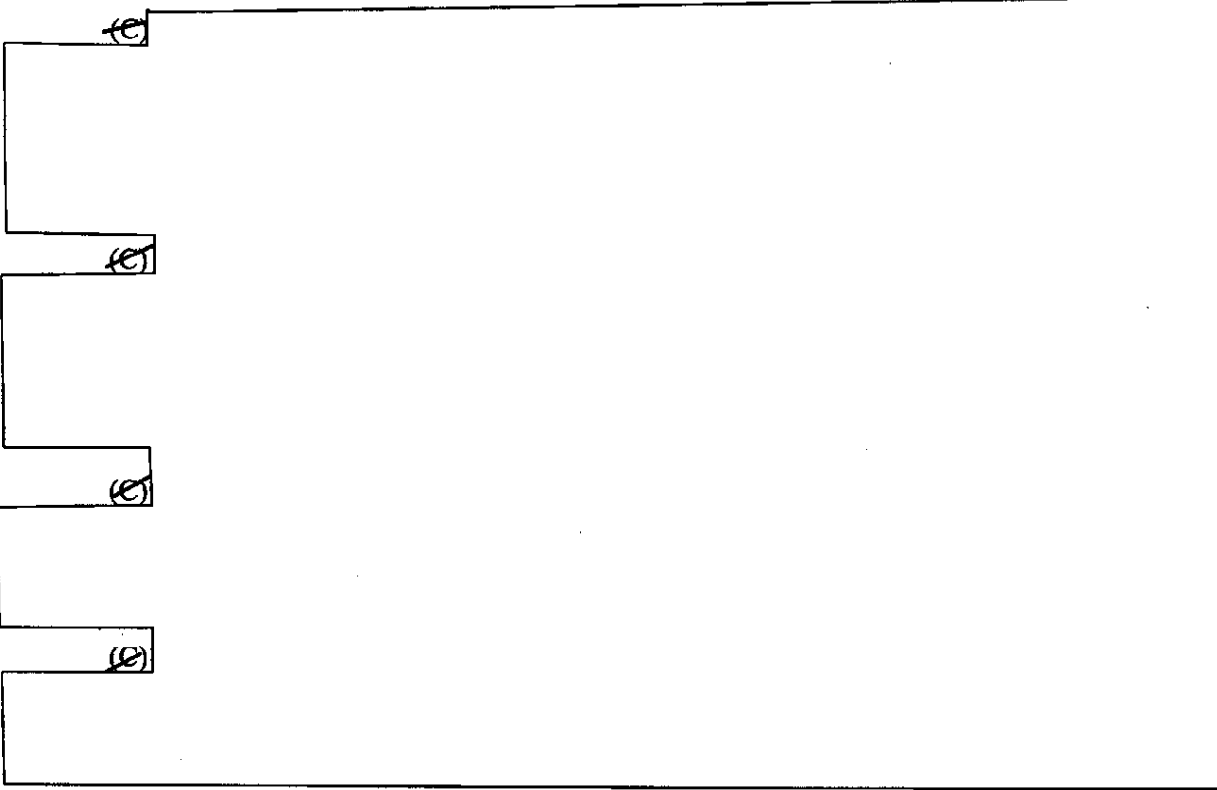
(U) Foreign Intelligence. The term "foreign intelligence" includes both positive foreign intelligence and counterintelligence.



~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

(U) Interception. The term "interception" means the acquisition by the United States Signals Intelligence System through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligence form but not including the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signal without reference to the information content carried by the signal.



(U) Technical Data Base. The term "technical data base" means information retained for cryptanalytic or traffic analytic purposes.

(U) Transiting Communications. The term "transiting communications" includes all communications that neither originate nor terminate in the United States, but which transit the United States during transmission.

(U) United States Person. For purposes of intentionally collecting the communications of a particular person, the term "United States person," in addition to the meaning in the Appendix to DoD Regulation 5240.1-R, includes any alien known to be presently in the United States; any unincorporated association of such aliens or American citizens; the United States operations, office, branch, or representative of a corporation incorporated abroad; any corporation or corporate subsidiary incorporated in the United States; and any U.S. flag non-

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -P.L. 86-36

~~SECRET//COMINT//X1~~

governmental aircraft or vessel: Provided, however, that the term "U.S. person" shall not include

[Redacted]

or (ii) a foreign power or powers as defined in Section 101 (a)(1)-(3) of FISA.

Sec. 3: Policy (U)

(U) The Director, National Security Agency, is assigned responsibility for signals intelligence collection and processing activities and communications security activities. In order to assure that these activities are conducted in accordance with the provisions of Executive Order 12333, the Director, or his designee, will issue appropriate directives and instructions implementing these procedures and governing the conduct of the United States Signals Intelligence System and the activities of communications security entities.

~~(S)~~ It is the policy of the United States Signals Intelligence System to collect, retain, and disseminate foreign communications and military tactical communications. It is recognized, however, that the United States Signals Intelligence System may incidentally intercept non-foreign communications, including those of or concerning United States persons, in the course of authorized collection of foreign communications. The United States Signals Intelligence System makes every reasonable effort, through surveys and technical means, to reduce to the maximum extent possible the number of such incidental intercepts acquired in the conduct of its operations. Information derived from these incidentally intercepted non-foreign communications may be disseminated to the Federal Bureau of Investigation when the information is foreign intelligence or counterintelligence or indicates a threat to the physical safety of any person. Dissemination of such information is also governed by these procedures and applicable minimization procedures approved in accordance with FISA. Specific communications sent from or intended for receipt by the United States persons are not intercepted deliberately by the United States Signals Intelligence System unless specific authorization for such interception has been obtained in accordance with these procedures.

~~(S//SI)~~ The President has authorized, and the Attorney General hereby specifically approves, interception by the United States Signals Intelligence System of:

[Redacted]

(b) (1)  
(b) (3) -50 USC 403  
(b) (3) -P.L. 86-36

\* United States and Allied Military exercise communications;

\* Signals collected during the search of the signals environment for foreign communications that may be developed into sources of signals intelligence;

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

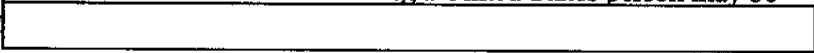
\* Signals collected during the monitoring of foreign electronic surveillance activities directed at United States communications consistent with the Foreign Intelligence Surveillance Act of 1978; and


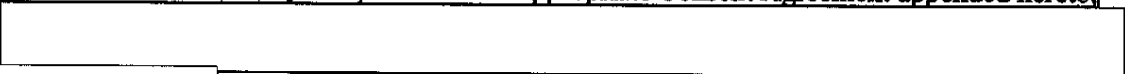
\* Signals collected during the testing and training of personnel in the use of signals intelligence collection equipment in the United States consistent with the Foreign Intelligence Surveillance of 1978.

Sec. 4: Procedures (U)



1. Collection

(a) ~~(S//SI)~~ Communications of or concerning a United States person may be intercepted intentionally only: 

(1) with the consent of such United States person. Where a United States person has consented, by completion of the appropriate Consent Agreement appended hereto,   


 or

(2) with specific prior court order pursuant to the Foreign Intelligence Surveillance Act of 1978 where applicable. All United States Signals Intelligence System requests for such court orders or approvals shall be forwarded by the Director, National Security Agency for certification by the Secretary of Defense or the Deputy Secretary of Defense (in case of the unavailability of both of these officials and in emergency situations, certification may be granted by another official authorized by executive order to certify such requests), and thence to the Attorney General; or

(3) with the specific prior approval of the Director, National Security Agency, in any case in which the United States person is reasonably believed to be held captive by a foreign power or by a group engaged in international terrorist activities. The Attorney General will be notified when the Director authorizes selection of communications concerning a United States person pursuant to this provision; or

(4) with specific prior approval by the Attorney General based on a finding by the Attorney General that there is probable cause to believe the United States person is an agent of a foreign power and that the purpose of the interception or selection is to collect significant

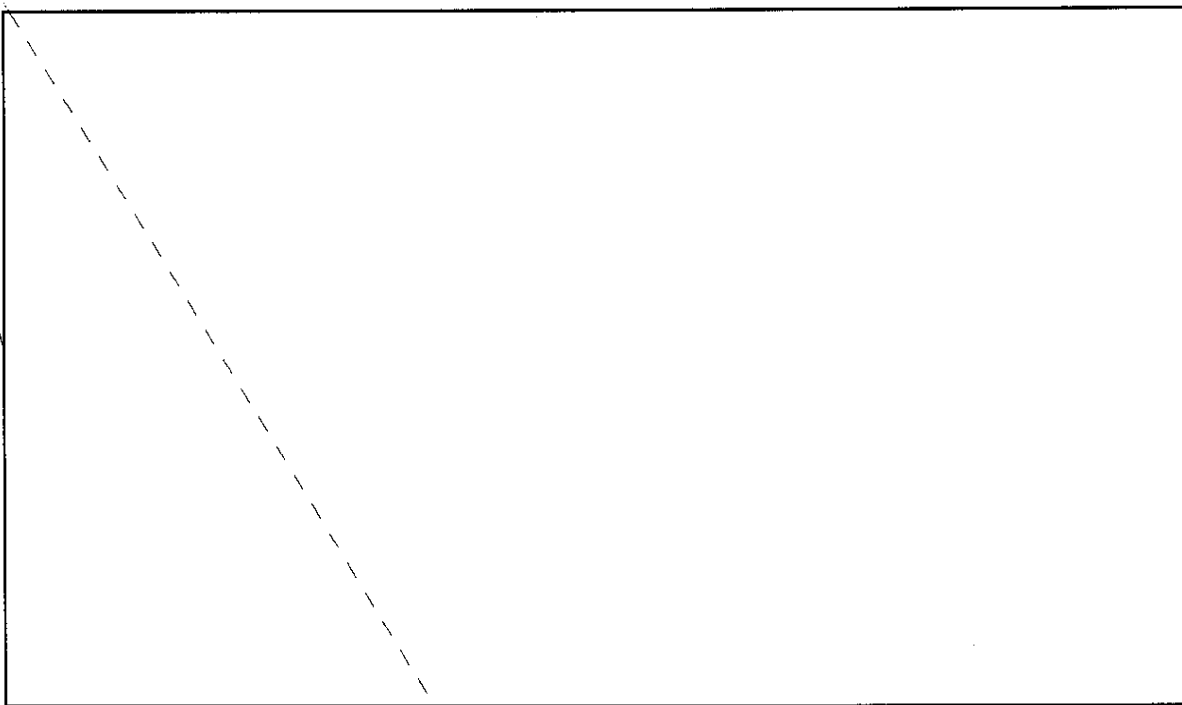
Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

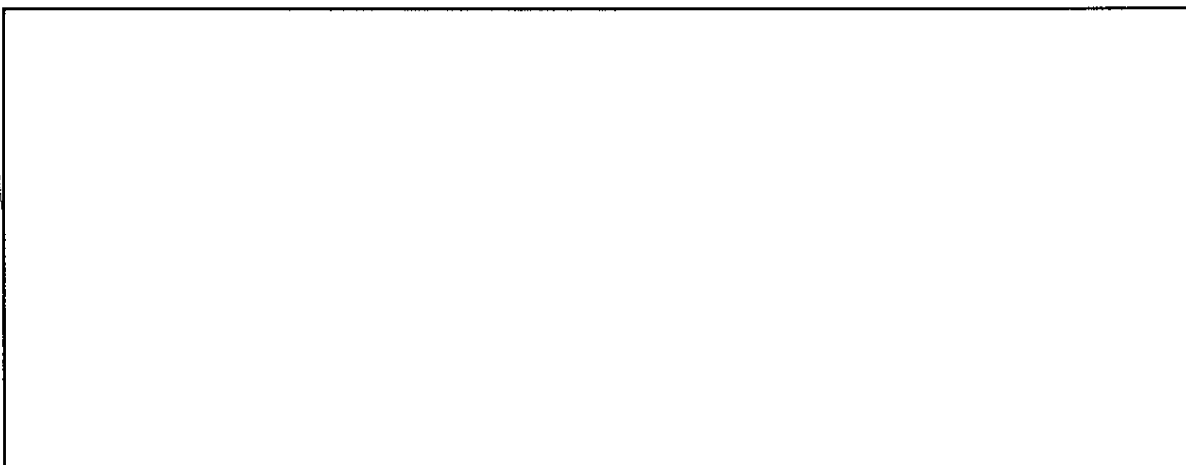
(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - P.L. 86-36

foreign intelligence. Such approvals shall be limited to a period of time not to exceed ninety days for individuals and one year for entities.



(d) ~~(S//SI)~~ Emergencies:

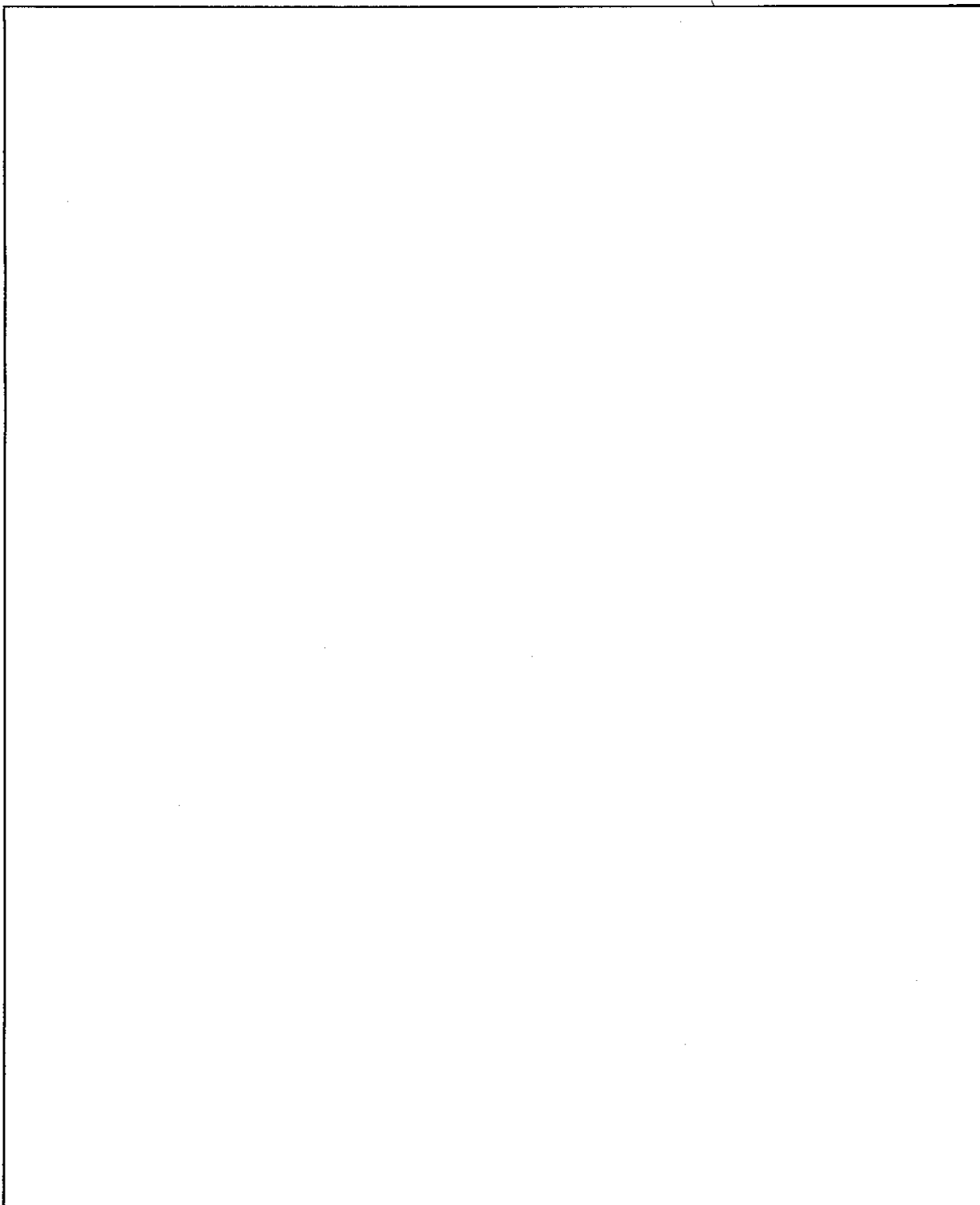
(1) The emergency provision in Section D of Part 2, Procedure 5, of DoD 5240.1-R, may be employed to authorize  communications of, or concerning, a United States persons defined in the Appendix to DoD Regulation 5240.1-R, when that person is outside the United States.



Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~



Annex to Policy 1-23  
Dated: 11 March 2004

A-7

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~



2. Retention (U)

~~(S//SI)~~ Foreign communications of, or concerning, United States persons that are intercepted by the United States Signals Intelligence System may be retained in their original form or as transcribed only:

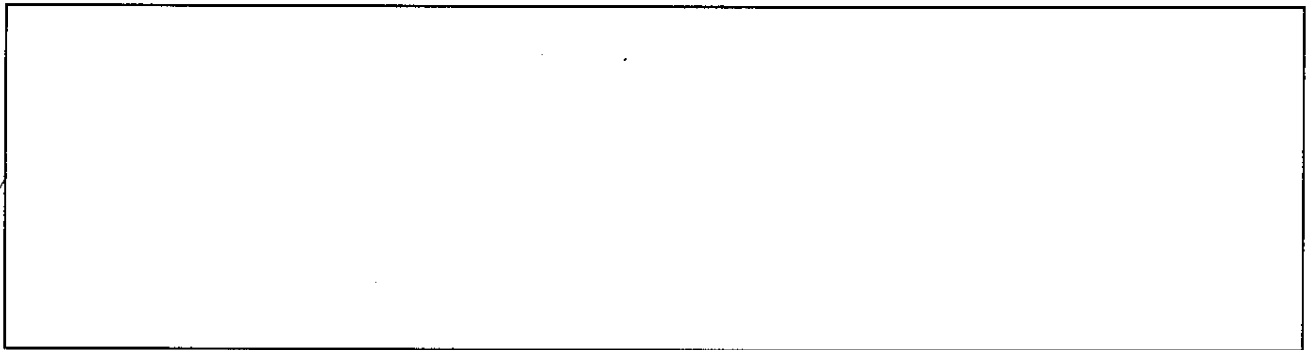
(a) if processed so as to eliminate any reference to United States persons;

(b) if necessary to the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future intelligent requirement. Sufficient duration may vary with the nature of the exploitation. In the context of a cryptanalytic effort, sufficient duration may consist of a period of time during which encrypted material is subject to, or of use in, cryptanalysis. In the case of international commercial communications that may contain the identity of United States persons and that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, National Security Agency, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or

(c) if dissemination of such communications without elimination of references to such United States persons would be permitted under section 4.A.4 below.

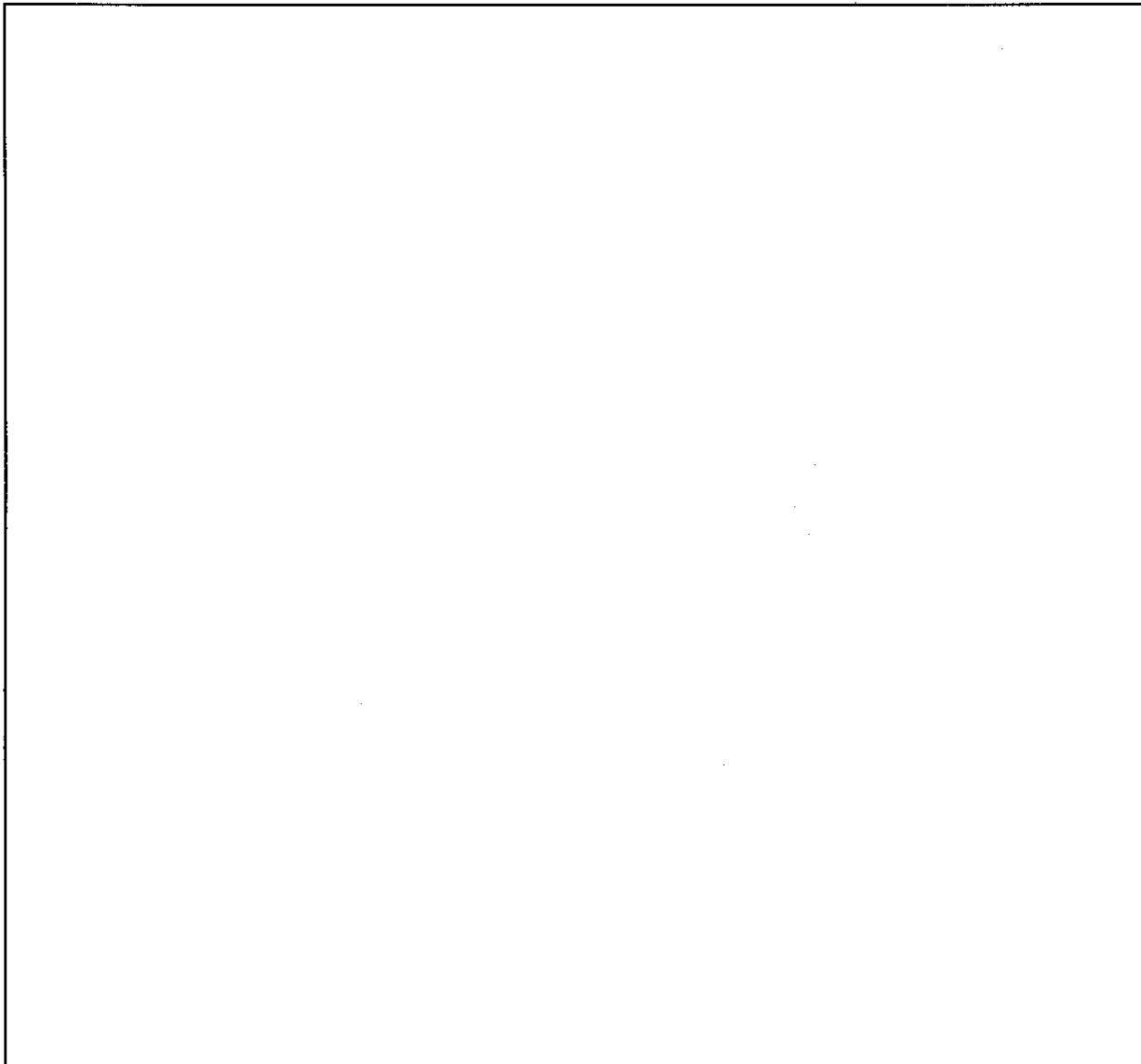
3. Processing (U)

(a) ~~(S//SI)~~ Foreign communications of, or concerning, United States persons must be processed in accordance with the following limitations:



~~SECRET//COMINT//X1~~



~~SECRET//COMINT//X1~~

#### 4. Dissemination (U)

~~(C//SI)~~ Dissemination of signals intelligence derived from foreign communications of, or concerning, United States persons is governed by Procedure 4 of DoD Regulation 5240.1-R. Dissemination of signals intelligence shall be limited to authorized signals intelligence consumers in accordance with requirements and tasking established pursuant to Executive Order 12333. Dissemination of information that is not pursuant to such requirements or tasking that constitutes foreign intelligence or counterintelligence or that is otherwise authorized under Procedure 4 shall be limited to those departments or agencies that have subject matter responsibility. Dissemination of the identity of a United States person is authorized if it meets

Annex to Policy 1-23  
Dated: 11 March 2004

A-9

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

one of the following criteria, each of which is also deemed to meet the standard of "necessary to understand or assess" the importance of foreign intelligence information (otherwise, the identity of the United States person must be replaced by a generic term, e.g., United States citizen or United States corporation):

(a) The United States person has consented to the use of communications of or concerning him or her and has executed the applicable consent form;

(b) the information is available publicly;

(c) the identity of the United States person is that of a senior official in the Executive Branch. When this exemption is applied, the Deputy Director for Operations, National Security Agency, will ensure that domestic political or personal information is not retained or disseminated;

(d) the communication or information indicates that the United States person may be an agent of a foreign power;

(e) the communication or information indicates that the United States person may be:

(1) a foreign power as defined in Section 101 (a)(4) or (6) of FISA;

(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 or her 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 United States person has, or has had, access to information or material classified by the United States;

(f) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(g) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information;

(h) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(i) the interception of the United States person's communications was authorized by a court order issued pursuant to Section 105 of FISA or by Attorney General approval issued

Annex to Policy 1-23  
Dated: 11 March 2004

A-10

~~SECRET//COMINT//X1~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-P.L. 86-36

~~SECRET//COMINT//XI~~

pursuant to Section 4.A.1 of this annex and the communication may relate to the foreign intelligence or counterintelligence purpose of the surveillance;

(j) the communication or information indicates a possible threat to the safety of a person or organization, including those who are targets, victims, or hostages of international terrorist organizations;

(k) the communication or information indicates that the United States person may be engaged in international narcotics trafficking activities;

(l) 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; or

(m) the identity of the United States person is otherwise necessary to understand foreign intelligence or counterintelligence or assess its importance. Access to technical data bases will be restricted to signals intelligence collection and analytic personnel. Requests for access from other personnel or entities shall be referred to the Deputy Director for Operations, National Security Agency. Domestic communications in which all communicants are United States persons shall be disposed of upon recognition, provided that technical data concerning frequency and channel usage may be retained for collection avoidance purposes.

B. (C)

[Redacted]

C. (C)

[Redacted]

~~D. (C)~~ Signals Intelligence: Search and Development. The United States Signals Intelligence System may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

1. Collection. Signals may be collected only for the purpose of identifying those signals that:

(a) may contain information related to the production of foreign intelligence or counterintelligence;

(b) are enciphered or appear to contain secret meaning;

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//XI~~

(b) (1)  
(b) (3) - 50 USC 403  
(c) (3) - P.L. 86-36

~~SECRET//COMINT//X1~~

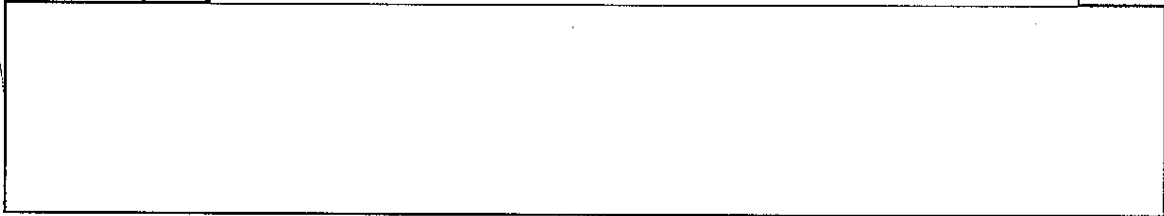
(c) are necessary to ensure efficient signals intelligence collection or to avoid the collection of unwanted signals; or

(d) reveal vulnerability of United States communications security.

2. Retention and Processing. Communications originating or intended for receipt in the United States, or originated or intended for receipt by United States persons, shall be processed in accordance with Section 4.A.3, provided that information necessary for cataloging the constituent elements of the signal environment may be produced and retained if such information does not identify a United States person. Information revealing a United States communications security vulnerability may be retained.

3. Dissemination. Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify United States persons, except that communication equipment nomenclature may be disseminated. Information that reveals a vulnerability of United States communications security may be dissemination to the appropriate security authorities.

E. (S//SI)



F. (U) Assistance to the Federal Bureau of Investigation.

1. In accordance with the provisions of Section 2.6 (c) of E.O. 12333, the National Security Agency may provide specialized equipment and technical knowledge to the Federal Bureau of Investigation to assist the Bureau in the conduct of its lawful functions. When requesting such assistance, The Federal Bureau of Investigation shall certify to the General Counsel, National Security Agency, that such equipment or technical knowledge is necessary to accomplishment of one or more of the Bureau's lawful functions.

2. The National Security Agency 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 Federal Bureau of Investigation shall certify to the General Counsel, National Security Agency, that such assistance is necessary to collect foreign intelligence or counterintelligence and that the approval of the Attorney General (and when necessary a order from a court of competent jurisdiction) has been obtained.

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

//s//  
William R. Taft  
DEPUTY SECRETARY OF DEFENSE  
26 April 1988

//s//  
Edwin Meese III  
ATTORNEY GENERAL  
27 May 1988

Annex to Policy 1-23  
Dated: 11 March 2004

A-13

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Executive Order 12333  
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 which may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only information which relates to the purpose stated above and is effective for the period:  
\_\_\_\_\_.

Signals intelligence reports containing information derived from communication so or from me may only be disseminated to me and to \_\_\_\_\_. Signals intelligence reports containing information derived from communication referencing me may only be disseminated to me and to [names of departments and agencies, e.g., DoD, CIA, etc] except as otherwise permitted by procedures under Executive Order 12333.

(SIGNATURE)  
(TITLE)

(UNCLASSIFIED until completed. Classify completed form based on information added, but not lower than CONFIDENTIAL.)

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

~~SECRET//COMINT//X1~~

Executive Order 12333  
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 which may relate to the purpose stated above.

Except as otherwise provided by Executive Order 12333 procedures, this consent covers only references to me in foreign communications and information derived there from which relates to the purpose stated above. This consent is effective for the period:  
\_\_\_\_\_.

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 [names of departments and agencies, e.g., DoD, CIA, etc] except as otherwise permitted by procedures under Executive Order 12333.

(SIGNATURE)  
(TITLE)

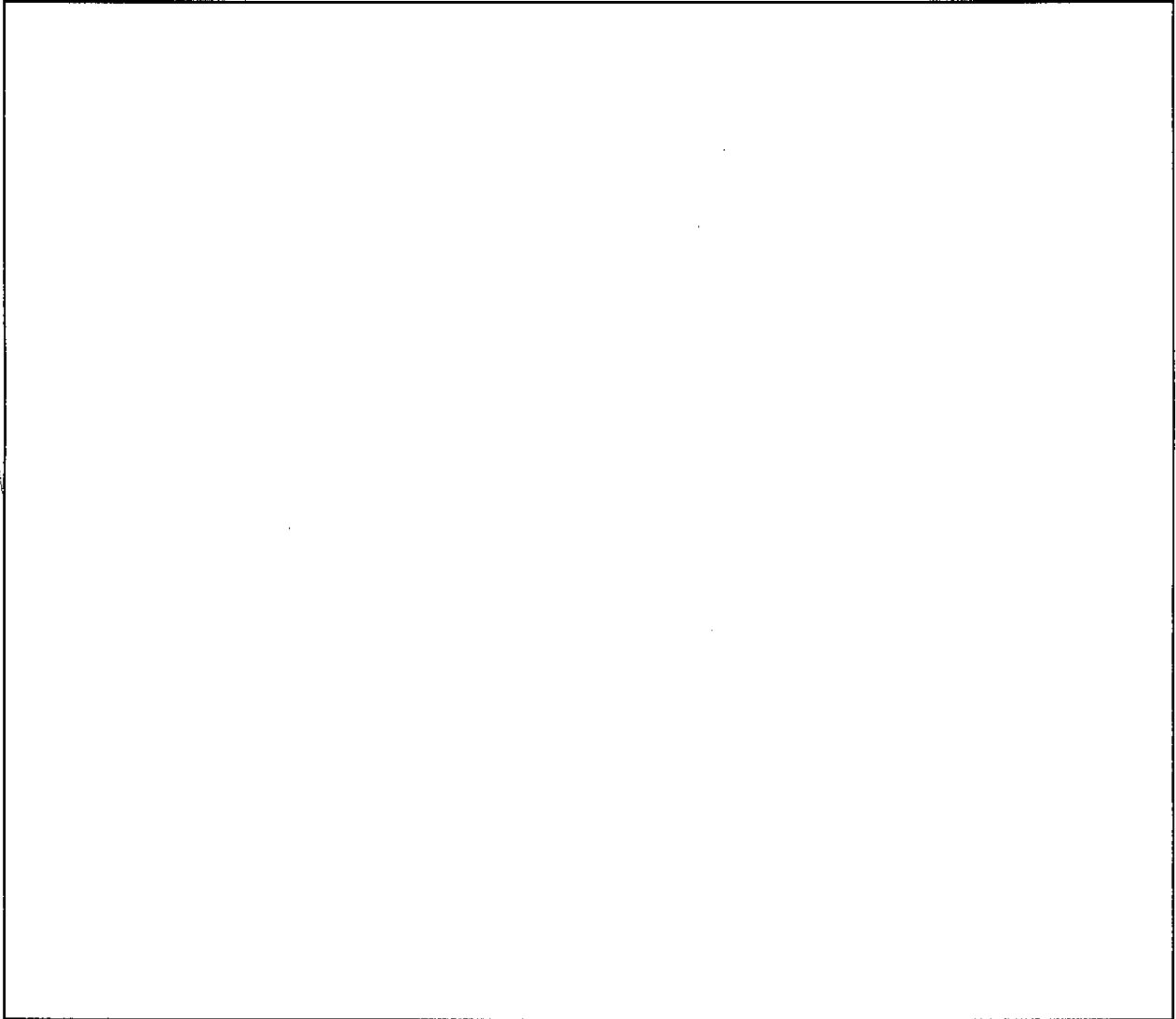
(UNCLASSIFIED until completed. Classify completed form based on information added, but not lower than CONFIDENTIAL.)

Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-P.L. 86-36

~~SECRET//COMINT//X1~~



Annex to Policy 1-23  
Dated: 11 March 2004

~~SECRET//COMINT//X1~~



**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE**

Fort George G. Meade, Maryland -

**UNITED STATES**

**SIGNALS INTELLIGENCE**

**DIRECTIVE**

**18**

**27 July 1993**

.....  
: See Letter of Promulgation for instructions on reproduction or release of this document. :  
.....

**OPC: [redacted] U1**

**CLASSIFIED BY NSA/CSSM 123-2**

**DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED**

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

Approved for Release by NSA on  
09-20-2006, FOIA Case # 9183

~~SECRET~~

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

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND  
MINIMIZATION PROCEDURES (FOUO)

LETTER OF PROMULGATION

(U) This USSID 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 of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18 and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 19.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS (Attention: [redacted] NSTS 963-3121 or STU III 688-5015).

*J.M. McConnell*

J. M. McCONNELL  
Vice Admiral, U.S. Navy  
Director

(b) (3)-P.L. 86-36 (b) (3)-P.L. 86-36

CLASSIFIED BY NSA/CSSM 123-2  
DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~



~~CONFIDENTIAL~~

USSID 18  
CHANGE 1  
28 October 1997

### DISTRIBUTION

1	C525	5	M422
1	CMATT	10	M423
1	DDO C/S	5	M43
1	DDO CIO	5	M431
1	DOD/IG	5	M432
1	G622	15	M441
3	G63	17	M442
1	G633	1	M4422
1	G72	1	M5
1	G732	20	M505
1	G7445	89	M52
1	G81	124	M53
1	G852	3	M54
1	G854	50	M543
1	H110	1	N22
1	H114	1	N5F
1	J63	1	N5F6
1	K253	3	P02
1	K41	1	P02 PLUS
1	K42	1	P021
1	K43	50	P0211/STOCK
1	K442	8	P0212
1	K442	8	P0213
1	K442	2	P0214
1	K442	3	P0216
1	K53	1	P022
1	K532	4	P023
1	L4C	1	P1
1	M05	1	P11
1	M051	1	P113
1	M052	1	P123
1	M1	3	P3
1	M11	2	P32
1	M12	1	P7
1	M13	1	F7 NSOC (ASGC)
1	M14	1	F7 NSOC (ESGC)
1	M15	1	F7 NSOC (NI/JIC)
1	M152	1	F7 NSOC (FO)
1	M153	1	F7 NSOC (WAGC)
1	M154	35	F761
1	M155	1	Q63
1	M156	2	Q631
1	M157	1	S3
1	M158	1	S312
1	M159	1	S332G
1	M2	1	S512/AC
1	M24	1	S541 (VRD)
1	M241	1	S542
1	M242	2	S8
1	M252	1	T09
1	M31	50	U
1	M32 (RMAC)	12	W65
1	M33	3	W652
1	M34	3	W6F
1	M342	22	W6F2
1	M35	21	W6F3
1	M36	16	W6F4
1	M421		



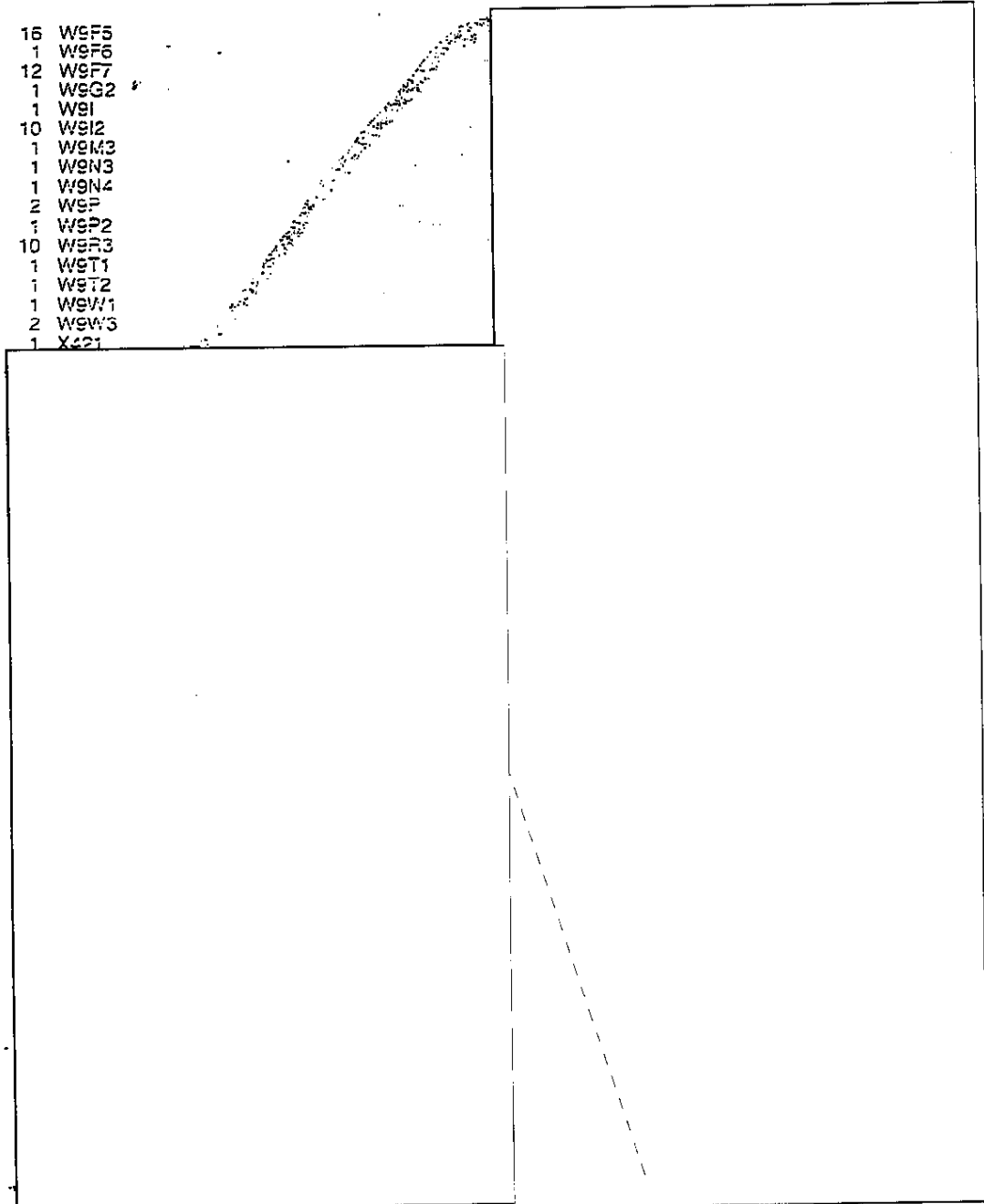
(b) (3)-P.L. 86- (b) (3)-P.L. 86-36

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

USSID 18  
CHANGE 1  
28 October 1997

- 16 W9F5
- 1 W9F6
- 12 W9F7
- 1 W9G2
- 1 W9I
- 10 W9I2
- 1 W9M3
- 1 W9N3
- 1 W9N4
- 2 W9P
- 1 W9P2
- 10 W9P3
- 1 W9T1
- 1 W9T2
- 1 W9W1
- 2 W9W3
- 1 X421

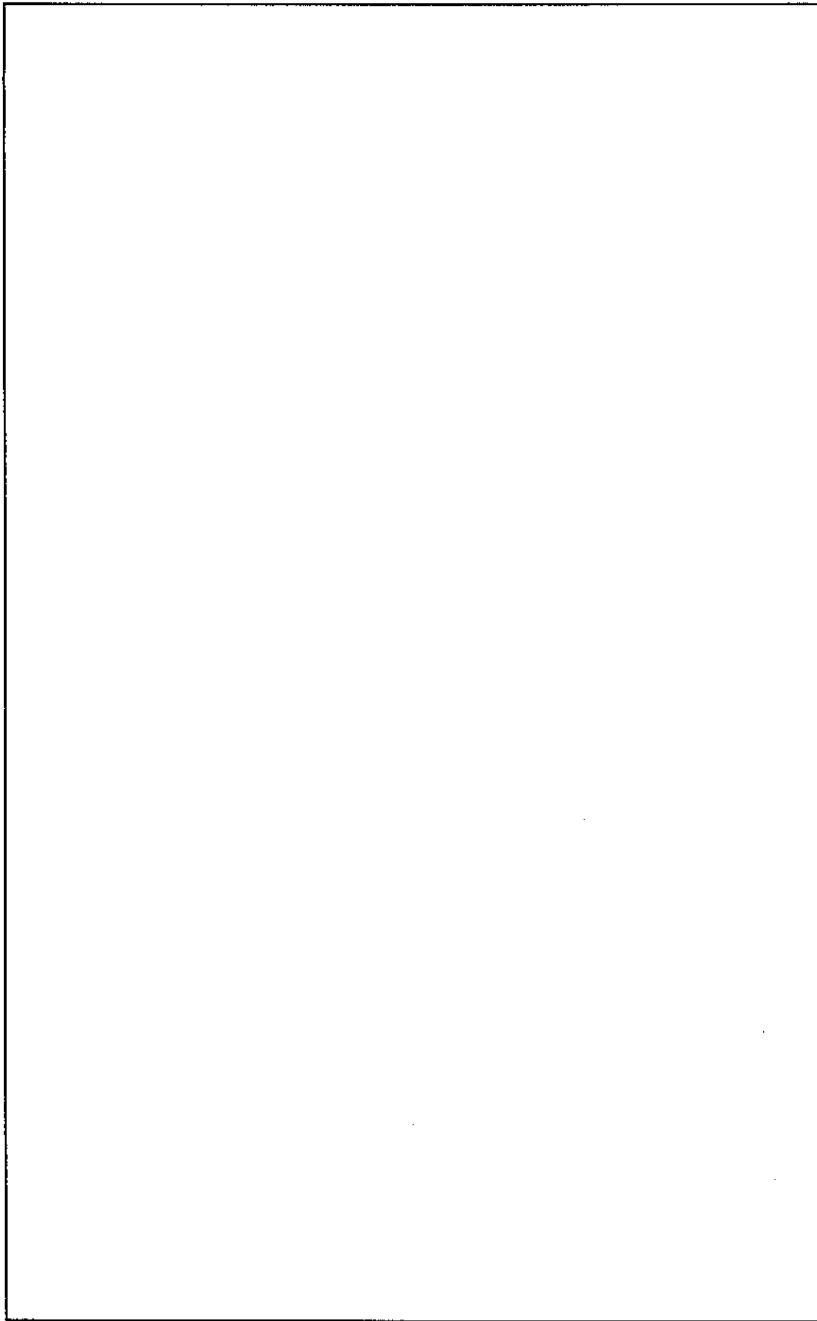


~~CONFIDENTIAL~~

(b) (3)-18 USC 798  
(b) (3)-50 USC 403

~~CONFIDENTIAL~~

USSID 18  
CHANGE 1  
28 October 1997

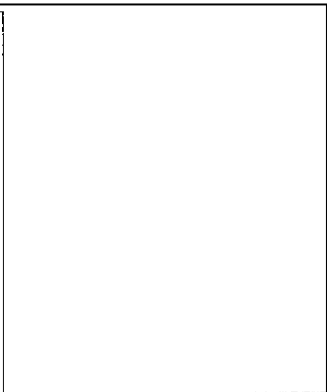
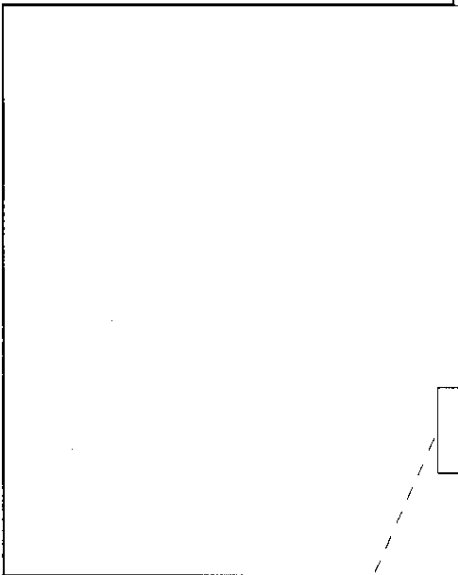


(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 795  
(b) (3) - P.L. 86-36

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

USSID 18  
CHANGE 1  
28 October 1997



DESTROY DISTRO PAGES AFTER  
POSTING CHANGE

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-P.L. 86-36  
(b) (3)-18 USC 798

~~CONFIDENTIAL~~

TABLE OF CONTENTS

SECTION 1 - PREFACE ..... 1

SECTION 2 - REFERENCES ..... 1

SECTION 3 - POLICY ..... 2

SECTION 4 - COLLECTION ..... 2

    4.1. Communications to, from or About U.S. Persons and [redacted] ..... 2

        to the United States

        a. Foreign Intelligence Surveillance Court Approval ..... 2

        b. Attorney General Approval ..... 2

        c. DIRNSA/CHCSS Approval ..... 2

        d. Emergency Situations ..... 3

        e. Annual Reports ..... 4

    4.2. [redacted] ..... 4

    4.3. Incidental Acquisition of U.S. Person Information ..... 4

        [redacted] ..... 5

        [redacted] ..... 5

        [redacted] ..... 5

        [redacted] ..... 5

    4.8. Distress Signals ..... 5

    4.9. COMSEC Monitoring and Security Testing of Automated Information Systems ..... 6

SECTION 5 - PROCESSING ..... 6

    5.1. [redacted] ..... 6

    5.2. Annual Review by DDO ..... 6

    5.3. Forwarding of Intercepted Material ..... 6

    5.4. Nonforeign Communications ..... 7

        a. Communications between Persons in the United States ..... 7

        b. Communications between U.S. Persons ..... 7

        c. Communications Involving an Officer or Employee of the U.S. Government ..... 7

        d. Exceptions ..... 7

    5.5. Radio Communications with a Terminal in the United States ..... 7

SECTION 6 - RETENTION ..... 8

    6.1. Retention of Communications to, from, or About U.S. Persons ..... 8

        a. Unenciphered Communications; and Communications Necessary to Maintain Technical Data Bases for Cryptanalytic or Traffic Analytic Purposes ..... 8

        b. Communications Which Could be Disseminated Under Section 7 ..... 8

    6.2. Access ..... 8

SECTION 7 - DISSEMINATION ..... 8

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-P.L. 86-36  
(b) (3)-18 USC 798



7.1. Focus of SIGINT Reports .....	8
7.2. Dissemination of U.S. Person Identities .....	9
a. Consent .....	9
b. Publicly Available Information .....	9
c. Information Necessary to Understand or Assess .....	9
7.3. Approval Authorities .....	10
a. DIRNSA/CHCSS .....	10
b. Field Units .....	10
c. DDO and Designees .....	10
7.4. Privileged Communications and Criminal Activity .....	10
7.5. Improper Dissemination .....	10
SECTION 8 - RESPONSIBILITIES .....	11
8.1. Inspector General .....	11
8.2. General Counsel .....	11
8.3. Deputy Director for Operations .....	12
8.4. All Elements of the USSS .....	12
SECTION 9 - DEFINITIONS .....	12
ANNEX A - PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U) .....	A/1
APPENDIX 1 - STANDARDIZED MINIMIZATION PROCEDURES FOR NSA SURVEILLANCES (ELECTRONIC) .....	A-1/1
ANNEX B - OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U) .....	B/1
ANNEX C - SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U) .....	C/1
ANNEX D - TESTING OF ELECTRONIC EQUIPMENT (U) .....	D/1
ANNEX E - SEARCH AND DEVELOPMENT OPERATIONS (U) .....	E/1
ANNEX F - [REDACTED] (U) .....	F/1
ANNEX G - TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT (U) .....	G/1
ANNEX H - CONSENT FORMS (U) .....	H/1
ANNEX I - [REDACTED] (S- <del>CGO</del> ) .....	I/1
ANNEX J - PROCEDURES FOR MONITORING RADIO COMMUNICATIONS OF SUSPECTED INTERNATIONAL NARCOTICS TRAFFICKERS (S- <del>CGO</del> ) (Issued separately to selected recipients) .....	J/1
ANNEX K - [REDACTED] (S- <del>CGO</del> ) .....	K/1

~~HANDLE VIA COMINT CHANNELS OF~~  
~~SECRET~~

(b) (1) -  
(b) (3) -50 USC 403  
(b) (3) -18 USC 798  
(b) (3) -P.L. 86-36

~~SECRET~~

27 July 1993

## USSID 18

LEGAL COMPLIANCE AND  
MINIMIZATION PROCEDURES (U)

## SECTION 1 - PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

## SECTION 2 - REFERENCES

## 2.1. (U) References

a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.

b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

**SECTION 3 - POLICY**

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.\* The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

**SECTION 4 - COLLECTION**

4.1. ~~(S-CCO)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] not be intentionally intercepted, [redacted]

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [redacted]

(c) Communications which are not to or from but merely about U.S. PERSONS, (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

\* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [redacted]

(4) [redacted]

(5) [redacted]

(a) A non-U.S. PERSON located outside the UNITED STATES, or

(b) [redacted]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

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

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

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

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

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER 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.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

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

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. ~~(S-CEO)~~

[Redacted]

a.

[Redacted]

b.

[Redacted]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36  
(b) (3)-50 USC 403

~~HANDLE VIA COMINT CHANNELS ONLY~~

4.4. ~~(S-CCO)~~ [Redacted]

a. [Redacted]

(1) [Redacted]

(2) [Redacted]

b. [Redacted]

c. [Redacted]

d. [Redacted]

4.5. ~~(S-CCO)~~ [Redacted]

a. [Redacted]

b. [Redacted]

4.6. ~~(S-CCO)~~ [Redacted]

4.7. ~~(S-CCO)~~ [Redacted]

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-F.L. 86-36  
(b) (3)-50 USC 403

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

(b)(1)  
(b)(3) - 50 USC 403  
(b)(7) - 18 USC 793  
(b)(3) - P.L. 86-36

SECTION 5 - PROCESSING

5.1. ~~(S-CCO)~~

[Redacted]

a.

[Redacted]

b.

[Redacted]

c.

[Redacted]

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a.

[Redacted]

b.

[Redacted]

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(S-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

5.4. ~~(S-CEO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

- (a) Establish or maintain intercept, or
- (b) Minimize unwanted intercept, or
- (c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

- (1) Significant FOREIGN INTELLIGENCE, or
- (2) Evidence of a crime or threat of death or serious bodily harm to any person, or
- (3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P95: PO2.

5.5. ~~(S-CEO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed [redacted] unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES, [redacted] may be processed [redacted] if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(b) (1)  
 (b) (3)-50 USC 40 (b) (1)  
 (b) (3)-18 USC 79 (b) (3)-50 USC 403  
 (b) (3)-P.L. 86-3 (b) (3)-18 USC 798  
 (b) (3)-P.L. 86-36 (b) (3)-P.L. 86-36



~~SECRET~~USSID 18  
27 July 1993

to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

## SECTION 6 - RETENTION

### 6.1. ~~(S-EGG)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-EGG)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

## SECTION 7 - DISSEMINATION

7.1. ~~(S-EGG)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P05. P02.

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-18 USC 793  
(b) (3)-2.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

~~SECRET~~USSID 18  
27 July 1993

7.2. ~~(C-CCC)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P05 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P05 should be in the form of a CRITICOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18  
27 July 1993

7.3. ~~(C-EEG)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P05, the Deputy Chief, P05, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(2) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P05 within 24 hours of discovery of the error.

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~



~~SECRET~~USSID 18  
27 July 1993**SECTION 8 - RESPONSIBILITIES**

8.1. (U) Inspector General. The Inspector General shall:

- a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.
- b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.
- c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.
- d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

8.2. (U) General Counsel. The General Counsel shall:

- a. Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures should be sent by CRITICOMM to DDI XDI, or by NSA/CSS secure telephone 963-3121, or STU III (301) 688-5015.
- b. Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.
- c. Advise the Inspector General in inspections and oversight of USSS activities.
- d. Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, Inspector General or Key Components Chief, all new major requirements and internally generated USSS activities.
- e. Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.
- f. Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.
- g. Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18  
27 July 1993

8.3. (U) Deputy Director for Operations (DDO). The DDO shall:

- a. Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.
- b. Apply the provisions of this USSID to all SIGINT production activities. The DDO staff focal point for USSID 18 matters is P85 (use CRITICOMM DDI XAO).  
PC2
- c. Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.
- d. Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the General Counsel. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the General Counsel prior to acceptance or execution.

8.4. (U) All Elements of the USSS. All elements of the USSS shall:

- a. Implement this directive upon receipt.
- b. Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: P85-  
PC2.
- c. Immediately inform the DDO of any tasking or instructions that appear to require actions at variance with this USSID.
- d. Promptly report to the NSA Inspector General and consult with the NSA General Counsel on all activities that may raise a question of compliance with this USSID:

## SECTION 9 - DEFINITIONS

9.1. ~~(S-CCO)~~ AGENT 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; or
- (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; or

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; or

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18  
27 July 1993

(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; or

(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 9.1.b.(1) through (3) or knowingly conspires with any person to engage in those activities.

c. For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. 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 provision, absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

9.2. ~~(C)~~ COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.

9.4. (U) COMMUNICATIONS ABOUT 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 mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

9.5. (U) CONSENT, for SIGINT purposes, means an 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.

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~USSID 18  
27 July 1993

b. In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

9.8. ~~(S)~~ FOREIGN COMMUNICATION means a communication that has at least one COMMICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

9.10. (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 UNITED STATES 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 UNITED STATES PERSONS, or

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

9.11. (U) 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 does not include 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.

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~





~~SECRET~~

USSID 18  
27 July 1993

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. Appear to be intended:

- (1) to intimidate or coerce a civilian population,
- (2) to influence the policy of a government by intimidation or coercion, or
- (3) to affect the conduct of a government by assassination or kidnapping, and

c. Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

9.13. (U) PUBLICLY AVAILABLE INFORMATION 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.

9.14. ~~(C)~~

[Redacted]

9.15. ~~(C)~~

[Redacted]

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the UNITED STATES exercises sovereignty.

9.18. ~~(C)~~ UNITED STATES PERSON:

- a. A citizen of the UNITED STATES,
- b. An alien lawfully admitted for permanent residence in the UNITED STATES,
- c. Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or
- d. CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - P.L. 86-36  
(b) (3) - 18 USC 798

~~SECRET~~USSID 18  
27 July 1993

e. The following guidelines 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 reasonably 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 is reasonably identified 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 (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(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.

(5) CORPORATIONS have the nationality of the nation-state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

~~SECRET~~USSID 18  
27 July 1993

**ANNEX A**  
**PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE**  
**SURVEILLANCE ACT (U)**

**SECTION 1 - PURPOSE AND APPLICABILITY**

1.1. (U) The Foreign Intelligence Surveillance Act (the Act) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. A complete copy of the Act is found at Annex B to NSA/CSS Directive 10-30. The Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States, all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy. The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General.

**SECTION 2 - GENERAL**

2.1. (U) Procedures and standards for securing Court orders or Attorney General certifications to conduct electronic surveillances are set forth in the Act. Requests for such orders or certifications should be forwarded by the appropriate Key Component through the NSA General Counsel to the Director, NSA/Chief, CSS and should be accompanied by a statement of the facts and circumstances justifying a belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which the surveillance will be directed are being used, or are about to be used, by that foreign power or agent. If the proposed surveillance meets the requirements of the Act and the Director approves the proposal, attorneys in the Office of the General Counsel will draw the necessary court application or request for Attorney General certification.

**SECTION 3 - MINIMIZATION PROCEDURES**

3.1. ~~(S-CEO)~~ Surveillances authorized by the Act are required to be carried out in accordance with the Act and pursuant to the court order or Attorney General certification authorizing that particular surveillance. In some cases, the court orders are tailored to address particular problems, and in those instances the NSA attorney will advise the appropriate NSA offices of the terms of the court's orders. In most cases, however, the court order will incorporate without any changes the standardized minimization procedures set forth in Appendix 1.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

A/1

~~SECRET~~

USSID 18 ANNEX A  
27 July 1993

**SECTION 4 - RESPONSIBILITIES**

4.1. (U) The General Counsel will review all requests to conduct electronic surveillances as defined by the Act, prepare all applications and materials required by the Act, and provide pertinent legal advice and assistance to all elements of the United States SIGINT System.

4.2. (U) The Inspector General will conduct regular inspections and oversight of all SIGINT activities to assure compliance with this Directive.

4.3. (U) All SIGINT managers and supervisors with responsibilities relating to the Act will ensure that they and their personnel are thoroughly familiar with the Act, its implementing procedures, and any court orders or Attorney General certifications pertinent to their mission. Personnel with duties related to the Act will consult the General Counsel's office for any required legal advice and assistance or training of newly assigned personnel. Appropriate records will be maintained demonstrating compliance with the terms of all court orders and Attorney General certifications, and any discrepancies in that regard will be promptly reported to the offices of the General Counsel and Inspector General.

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

APPENDIX 1

Standard Minimization Procedures for  
NSA Electronic Surveillances

Table of Contents

Section 1 — Applicability and Scope Section	A-1/2
Section 2 — Definitions	A-1/2
a. Acquisition	A-1/2
b. Communications concerning a U.S. Person	A-1/2
c. Communications of a U.S. Person	A-1/2
d. Consent	A-1/2
e. [Redacted]	A-1/2
f. Identification of a U.S. Person	A-1/3
g. [Redacted]	A-1/3
h. Publicly available information	A-1/3
i. Technical data base	A-1/3
j. U.S. person	A-1/3
Section 3 — Acquisition and Processing — General	A-1/3
a. Acquisition	A-1/3
b. Verification	A-1/3
c. Monitoring, Recording, and Processing	A-1/4
d. U.S. Persons Employed by the Foreign Power	A-1/4
e. Destruction of Raw Data	A-1/4
f. Non-Pertinent Communications	A-1/5
g. Change in Target's Location or Status	A-1/5
Section 4 — Acquisition and Processing — Special Procedures	A-1/5
a. Collection Against Residential Premises	A-1/5
b. Attorney-Client Communications	A-1/6
Section 5 — Domestic Communications	A-1/6
a. Dissemination	A-1/6
b. Retention	A-1/6
Section 6 — Foreign Communications of or Concerning U.S. Persons	A-1/7
a. Retention	A-1/7
b. Dissemination	A-1/7
Section 7 — Other Foreign Communications	A-1/8
Section 8 — [Redacted]	A-1/8

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36  
(b) (3)-50 USC 403

~~SECRET~~USSID 18 ANNEX A  
APPENDIX 1  
27 July 1993

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, DC  
STANDARDIZED MINIMIZATION  
PROCEDURES FOR NSA ELECTRONIC SURVEILLANCES

Pursuant to Section 101 (h) of the Foreign Intelligence Surveillance Act of 1978 (hereinafter "the Act"), the following procedures have been adopted by the Attorney General and shall be followed by the NSA in implementing this electronic surveillance: (U)

**SECTION 1 – APPLICABILITY AND SCOPE (U)**

These procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of the Act. These procedures also apply to non-United States persons where specifically indicated. (U)

**SECTION 2 – DEFINITIONS (U)**

In addition to the definitions in Section 101 of the Act, the following definitions shall apply to these procedures:

(a) Acquisition means the collection by NSA through electronic means  communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization shall be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among:

- (1) foreign powers;
- (2) officers and employees of foreign powers; or
- (3) a foreign power and officers or employees of a foreign power.

All other communications are domestic communications. ~~(S-EGG)~~

(b)(1)  
(b)(3)-50 USC 403  
(b)(3)-18 USC 798  
(b)(3)-P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(C1 - Oct 97)

~~SECRET~~USSID 18 ANNEX A  
APPENDIX 1  
27 July 1993

(f) Identification of a United States person means the name, unique title, address, or other personal identifier of a United States person in the context of activities conducted by that person or activities conducted by others that are 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, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S-CCO)~~

(g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

(h) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(i) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S-CCO)~~

(j) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

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

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

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with Title 8, United States Code, Section 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

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

### SECTION 3 -- ACQUISITION AND PROCESSING -- GENERAL (U)

#### (a) Acquisition (U)

The acquisition of information by electronic surveillance shall be made in accordance with the certification of the Attorney General or the court order authorizing such surveillance and conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance. ~~(S-CCO)~~

#### (b) Verification (U)

At the initiation of the electronic surveillance, the NSA or the Federal Bureau of Investigation, if providing operational support, shall verify that the communication lines or telephone numbers being targeted are the lines or numbers of the target authorized by court order or Attorney General certification. Thereafter, collection personnel will monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance. ~~(S-CCO)~~

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

(CI - Oct 97)



(c) Monitoring, Recording, and Processing (U)

(1) Electronic surveillance of the target may be monitored contemporaneously, recorded automatically, or both. (U)

(2) Personnel who monitor the electronic surveillance shall exercise reasonable judgement in determining whether particular information acquired must be minimized and shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either as clearly not relevant to the authorized purpose of the surveillance (e.g., the communication does not contain foreign intelligence information) or as containing evidence of a crime which may be disseminated under these procedures. ~~(S-CCO)~~

(3) Communications of or concerning United States persons that may be related to the authorized purpose of the surveillance may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, and 6 of these procedures. ~~(C)~~

(4) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S-CCO)~~

(5) Each communication shall be reviewed to determine whether it is a domestic or foreign communication to or from the targeted premises and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5 and 6 of these procedures. ~~(S-CCO)~~

(6) Magnetic tapes or other storage media containing foreign communications may be scanned to identify and select communications for analysis.

[Redacted]

(7) Further processing, retention and dissemination of foreign communications shall be made in accordance with Sections 4, 6, and 7, as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications shall be made in accordance with Sections 4 and 5 below. ~~(S-CCO)~~

(d) U.S. Persons Employed by the Foreign Power ~~(C)~~

Communications of or concerning United States persons employed by a foreign power may be used and retained as otherwise provided in these procedures except that:

(1) Such United States persons shall not be identified in connection with any communication that the person places or receives on behalf of another unless the identification is permitted under Section 6 of these procedures; and

(2) personal communications of United States persons that could not be foreign intelligence may only be retained, used, or disseminated in accordance with Section 5 of these procedures. ~~(S-CCO)~~

(e) Destruction of Raw Data ~~(C)~~

Communications and [Redacted] shall be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet such retention standards and that are known to contain communications of or concerning United States persons shall be promptly destroyed. ~~(S-CCO)~~

(b) (1)  
(b) (3)-50 USC 403  
(b) (3)-E.O. 86-36  
(b) (3)-18 USC 798

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(f) Non-pertinent Communications (U)

(1) Communications determined to fall within established categories of non-pertinent communications, such as those set forth in subparagraph (6) of this section, should not be retained unless they contain information that may be disseminated under Sections 5, 6, or 7 below. (U)

(2) Monitors may listen to all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be disseminated under Sections 5, 6, or 7 below. ~~(S-CCO)~~

(3) Communications of United States persons will be analyzed to establish categories of communications that are not pertinent to the authorized purpose of the surveillance. (U)

(4) These categories should be established after a reasonable period of monitoring the communications of the targets. (U)

(5) Information that appears to be foreign intelligence may be retained even if it is acquired as a part of a communication falling within a category that is generally non-pertinent. ~~(S-CCO)~~

(6) Categories of non-pertinent communications which may be applied in these surveillance include:

- (i) Calls to and from United States Government officials;
- (ii) Calls to and from children;
- (iii) Calls to and from students for information to aid them in academic endeavors;
- (iv) Calls between family members; and
- (v) Calls relating solely to personal services, such as food orders, transportation,

etc. ~~(S-CCO)~~

(g) Change in Target's Location or Status ~~(S-CCO)~~

(1) During periods of known extended absence by a targeted agent of a foreign power from premises under surveillance, only communications to which the target is a party may be retained and disseminated. ~~(S-CCO)~~

(2) When there is reason to believe that the target of an electronic surveillance is no longer a foreign power or an agent of a foreign power, or no longer occupies the premises authorized for surveillance, that electronic surveillance shall be immediately terminated, and shall not resume unless subsequently approved under the Act. When any person involved in collection or processing of an electronic surveillance being conducted pursuant to the Act becomes aware of information tending to indicate a material change in the status or location of a target, the person shall immediately ensure that the NSA's Office of General Counsel is also made aware of such information. ~~(S-CCO)~~

**SECTION 4 - ACQUISITION AND PROCESSING - SPECIAL PROCEDURES (U)**

(a) Collection Against Residential Premises ~~(S-CCO)~~

(1) An electronic surveillance directed against premises located in the United States and used for residential purposes shall be conducted by technical means designed to limit the information acquired to communications that have one communicant outside the United States.

The technical means employed shall consist of

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(C1 - Oct 97)

(b) (1)  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36  
(b) (3) - 50 USC 403

[redacted] known to be used by the targeted foreign power and its agents. Communications to or from the target residential premises that are processed [redacted] located in a foreign country, or on the foreign country or foreign city telephone direct dialing codes (area codes) for the areas in which such foreign powers or agents are located. ~~(S-CCO)~~

(2) [redacted]

[redacted] ~~(S-CCO)~~

(3) Domestic communications that are incidentally acquired during collection against residential premises shall be handled under Section 5 of these procedures. ~~(S-CCO)~~

(b) Attorney-Client Communications ~~(S)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication shall be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the tape containing that conversation will be placed under seal and the Department of Justice, Office of Intelligence Policy and Review, shall be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. ~~(S-CCO)~~

**SECTION 5 - DOMESTIC COMMUNICATIONS (U)**

(a) Dissemination (U)

Communications identified as domestic communications shall be promptly destroyed, except that:

(1) domestic communications that are reasonably believed to contain foreign intelligence information shall be disseminated to the Federal Bureau of Investigation (including United States person identities) for possible further dissemination by the Federal Bureau of Investigation in accordance with its minimization procedures;

(2) domestic communications that do not contain foreign intelligence information, but that are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed, shall be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General; and

(3) domestic communications that are reasonably believed to contain technical data base information, as defined in Section 2(f), may be disseminated to the Federal Bureau of Investigation and to other elements of the U.S. SIGINT system. ~~(S-CCO)~~

(b) Retention (U)

(1) Domestic communications disseminated to Federal law enforcement agencies may be retained by the NSA for a reasonable period of time, not to exceed six months (or any shorter period set by court order), to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes. ~~(S-CCO)~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

~~SECRET~~USSID 18 ANNEX A  
APPENDIX I  
27 July 1993

(2) Domestic communications reasonably believed to contain technical data base information may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S-CCO)~~

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S-CCO)~~

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements. ~~(S-CCO)~~

## SECTION 6 - FOREIGN COMMUNICATIONS OF OR CONCERNING UNITED STATES PERSONS (U)

### (a) Retention (U)

Foreign communications of or concerning United States persons acquired by the NSA in the course of an electronic surveillance subject to these procedures may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. in the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S-CCO)~~

### (b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~SECRET~~

USSID 18 ANNEX A  
APPENDIX 1  
27 July 1993

(3) the communication or information indicates that the United States person may be:

- (A) an agent of a foreign power;
- (B) a foreign power as defined in Section 101(a)(4) or (6) of the Act;
- (C) residing outside the United States and holding an official position in the government or military forces of a foreign power;
- (D) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
- (E) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material.

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States 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;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States 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;

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General. (U)

**SECTION 7 - OTHER FOREIGN COMMUNICATIONS (U)**

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

**SECTION 8 - [REDACTED] (S-CCO)**

- (a) [REDACTED] (S-CCO)
- (b) [REDACTED] (S-CCO)
- (c) [REDACTED] (S-CCO)
- (d) [REDACTED] (S-CCO)

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

(b) (1)  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36  
(b) (3) - 50 USC 403

~~SECRET~~

USSID 18 ANNEX A  
APPENDIX 1  
27 July 1993

[Redacted]

(S-669)

Approved by Attorney General Janet Reno on 1 July 1997

- (b) (1)
- (b) (3)-18 USC 798
- (b) (3)-P.L. 86-36
- (b) (3)-50 USC 403

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

(C1 - Oct 97)

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

**SECTION 1 - GENERAL**

1.1. (U) In accordance with the provisions of Section 2.6 of E.O. 12333, and the NSA/FBI Memorandum of Understanding of 25 November 1980, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the FBI in the conduct of its lawful functions. When requesting such assistance, the FBI will certify to the General Counsel of NSA that such equipment or technical knowledge is necessary to the accomplishment of one or more of the FBI's lawful functions.

1.2. (U) NSA may also provide expert personnel to assist FBI personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence. When requesting the assistance of expert personnel, the FBI will certify to the General Counsel that such assistance is necessary to collect foreign intelligence 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, Deputy Director, NSA, the Deputy Director for Operations, or the Deputy Director for Technology and Systems. The Deputy Director for Operations and the Deputy Director for Technology and Systems may approve requests for such assistance only with the concurrence of the General Counsel.

~~FOR OFFICIAL USE ONLY~~

B/1

---

~~CONFIDENTIAL~~USSID 18  
27 July 1993

## ANNEX C

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

## SECTION 1 - POLICY

1.1. ~~(S)~~ 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). Joint Chiefs of Staff Memorandum MICS111-88, 18 August 1988, and USSID 4, 16 December, 1988, establish 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) The term "Military Tactical Communications" means 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. ~~(S)~~ <sup>(e)</sup> The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S. persons. (c2)

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, provided that a record describing the signal or frequency user in technical and generic terms may be retained for signal identification and Collection-avoidance purposes. Inadvertently intercepted communications that contain anomalies in enciphered communications that reveal a potential vulnerability to United States communications security should be forwarded to the NSA Deputy Director for Information Systems Security.

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~

USSID 18 ANNEX C  
27 July 1993

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

~~CONFIDENTIAL~~

**ANNEX D**  
**TESTING OF ELECTRONIC EQUIPMENT (U)**

**SECTION 1 - PURPOSE AND APPLICABILITY**

1.1. (U) This Annex applies to the testing of electronic equipment that has the capability to intercept communications and other non-public information. Testing includes development, calibration, and evaluation of such equipment, and will be conducted, to the maximum extent practical, without interception or monitoring of U.S. persons.

**SECTION 2 - PROCEDURES**

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

a. To the maximum extent practical, the following should be used:

- (1) Laboratory-generated signals,
- (2) Communications transmitted between terminals located outside the United States not used by any known U.S. person,
- (3) Official government agency communications with the consent of an appropriate official of that agency, or an individual's communications with the consent of that individual,
- (4) Public broadcast signals, or
- (5) Other communications in which there is no reasonable expectation of privacy (as approved in each instance by the NSA General Counsel).

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

- (1) the proposed test is coordinated with the NSA General Counsel;
- (2) the test is limited in scope and duration to that necessary to determine the capability of the equipment;
- (3) no particular person is targeted without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and
- (4) the test does not exceed 90 calendar days.

~~FOR OFFICIAL USE ONLY~~

c. Where the test involves communications other than those identified in 2.1 .a. and a test period longer than 90 days is required, the Foreign Intelligence Surveillance Act requires that the test be approved by the Attorney General. Such proposals and plans shall be submitted by USSS elements through the General Counsel, NSA, to the Director, NSA/Chief, CSS 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 other than communications between non-U.S. persons outside the United States which are acquired during a test and evaluation shall be:

a. retained and used 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 before or immediately 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.

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~USSID 18  
27 July 1993

## ANNEX E

## SEARCH AND DEVELOPMENT OPERATIONS (U)

## SECTION 1 - PROCEDURES

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

1.2. ~~(S-CCO)~~ The USSS may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

a. Signals may be collected only for the purpose of identifying those signals that:

(1) may contain information related to the production of foreign intelligence or counterintelligence;

(2) are enciphered or appear to contain secret meaning;

(3) are necessary to assure efficient signals intelligence collection or to avoid the collection of unwanted signals; or,

(4) reveal vulnerabilities of United States communications security.

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 5 of USSID 18, provided that information necessary for cataloging the constituent elements of the signal environment may be processed and retained if such information does not identify a U.S. person. Information revealing a United States communications security vulnerability may be retained.

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. 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.

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~

~~CONFIDENTIAL~~

USSID 18  
27 July 1993

ANNEX F

[Redacted] (C)

SECTION 1 - PROCEDURES

1.1. (C) [Redacted]

1.2. (C) [Redacted]

(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-P.L. 06-36  
(b) (3)-50 USC 403

~~CONFIDENTIAL~~

**ANNEX G**

**TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT  
COLLECTION AND OTHER SURVEILLANCE EQUIPMENT (U)**

**SECTION 1 - APPLICABILITY**

1.1. (U) This Annex applies to all USSS use of SIGINT collection and other surveillance equipment for training purposes.

**SECTION 2 - POLICY**

2.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment shall be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons or persons in the United States who have not given consent to such interception. Communications and information protected by the Foreign Intelligence Surveillance Act (FISA) (see Annex A) will not be collected for training purposes.

**SECTION 3 - PROCEDURES**

3.1. (U) The training of USSS personnel in the operation and use of SIGINT collection and other surveillance equipment shall include guidance concerning the requirements and restrictions of the FISA, Executive Order 12333, and USSID 18.

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

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

b. The contents of private communications of nonconsenting U.S. persons may not be acquired 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.

3.3. (U) The limitations in paragraph 3.2. 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; and

~~FOR OFFICIAL USE ONLY~~

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

3.4. (U) Information collected during training that involves authorized intelligence targets may be retained in accordance with Section 6 of USSID 18 and disseminated in accordance with Section 7 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.

~~FOR OFFICIAL USE ONLY~~

**ANNEX H**  
**CONSENT FORMS (U)**

**SECTION 1 - PURPOSE**

1.1. (U) The forms set forth in this Annex are for use in recording consent by U.S. persons for USSS elements to collect and disseminate foreign communications concerning that person. The first form is consent to collect and disseminate a U.S. person's communications as well as references to that person in foreign communications. The second form is consent to collect and disseminate only references to the U.S. person and does not include communications to or from that person.

1.2. (U) Section 4.1.c. of USSID 18 states that the Director, NSA/Chief, CSS has authority to approve the consensual collection of communications to, from or about U.S. persons. Elements of the USSS proposing to conduct consensual collection should forward a copy of the executed consent form and any pertinent information to the Director, NSA/Chief, CSS for approval.

1.3. (U) The forms provided on the following pages may be reproduced, provided the security classifications (top and bottom) are removed. It is the responsibility of the user to properly reclassify the document in accordance with requisite security guidelines.

~~FOR OFFICIAL USE ONLY~~



~~SECRET~~

USSID 18 ANNEX H  
27 July 1993

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, \_\_\_\_\_, 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 12333 procedures, this consent covers only information that relates to the purpose stated above and is effective for the period to \_\_\_\_\_

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 12333.

\_\_\_\_\_  
(SIGNATURE)

\_\_\_\_\_  
(TITLE)

\_\_\_\_\_  
(DATE)

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET~~

USSID 18 ANNEX H  
27 July 1983

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, \_\_\_\_\_, 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 12333 procedures, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period \_\_\_\_\_ to \_\_\_\_\_

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 12333.

\_\_\_\_\_  
(SIGNATURE)

\_\_\_\_\_  
(TITLE)

\_\_\_\_\_  
(DATE)

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

~~SECRET~~

USSID 18  
27 July 1993

ANNEX I

[Redacted] (S-CCO)

[Redacted]

[Redacted]

(b) (1)  
(b) (3) - P.L. 86-36  
(b) (3) - 18 USC 798  
(b) (3) - 50 USC 403

[Redacted]

(S-CCO) [Redacted]

[Redacted]

[Redacted]

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~SECRET - COMINT CHANNELS~~



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

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

24 April 1986

USSID 18

ANNEX J

PROCEDURES FOR MONITORING RADIO  
COMMUNICATIONS OF SUSPECTED  
INTERNATIONAL NARCOTICS  
TRAFFICKERS ~~(FOUO)~~

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36

OPC: D2

---

LETTER OF PROMULGATION

~~(S-CCO)~~ This Annex implements Sections 2.3. and 2.6.(b) of Executive Order 12333, Sections 372 and 374 of Title 10, United States Code, and special Attorney General procedures.

(U) If this edition is not needed, destroy it and notify DIRNSA/CHCSS (P0442, USSID Manager) of the destruction and pertinent details. Also, notify P0442 if this document is destroyed because of an emergency action.

(U) The authority for approving requests for the reproduction or the removal of any portion of this USSID for use within the United States SIGINT System rests solely with the USSID Manager or the local

Designated USSID Representative. Any other reproduction or removal of parts of this document is prohibited.



(b) (3) - P.L. 86-36

WILLIAM E. ODOM  
Lieutenant General, USA  
Director, NSA/Chief, CSS

---

**TABLE OF CONTENTS**

**SECTION 1 - PURPOSE AND SCOPE**

**SECTION 2 - DEFINITIONS**

**SECTION 3 - COLLECTION**

**SECTION 4 - RETENTION**

**SECTION 5 - DISSEMINATION**

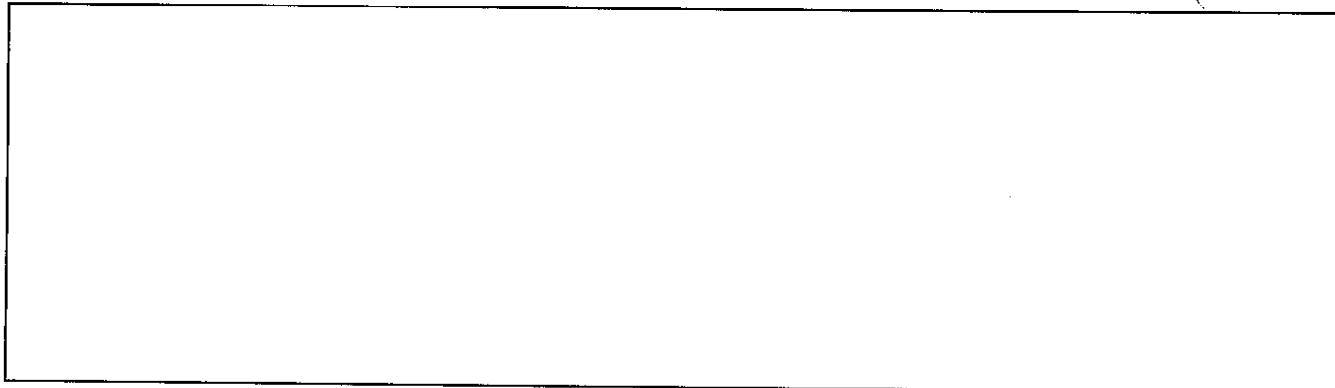
**SECTION 6 - IDENTIFICATION OF U.S. PERSONS**

---

---

(b) (1)  
(b) (3) - 18 USC 798  
(b) (3) - P.L. 86-36  
(b) (3) - 50 USC 403

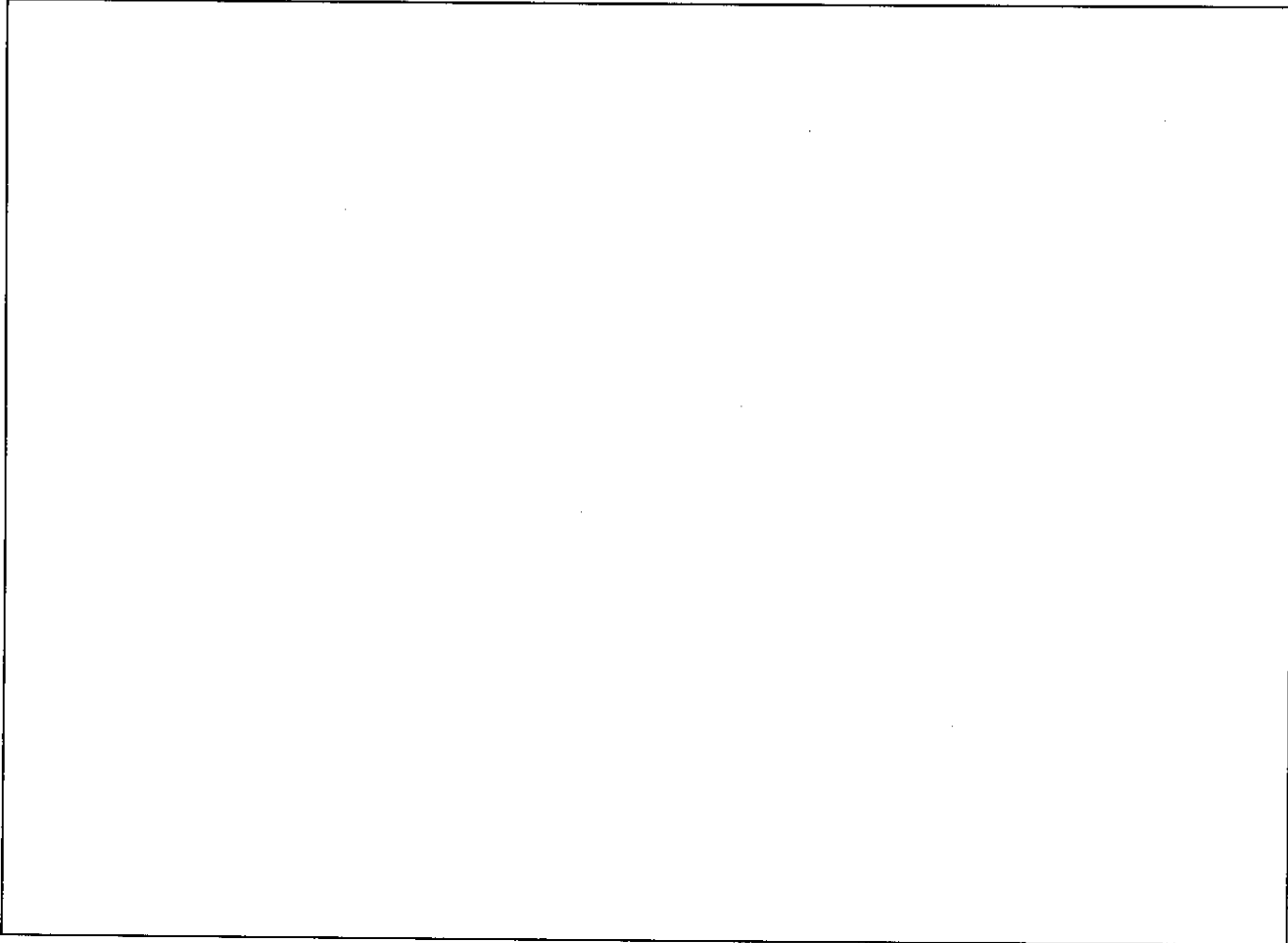
**SECTION 1 - PURPOSE AND SCOPE**



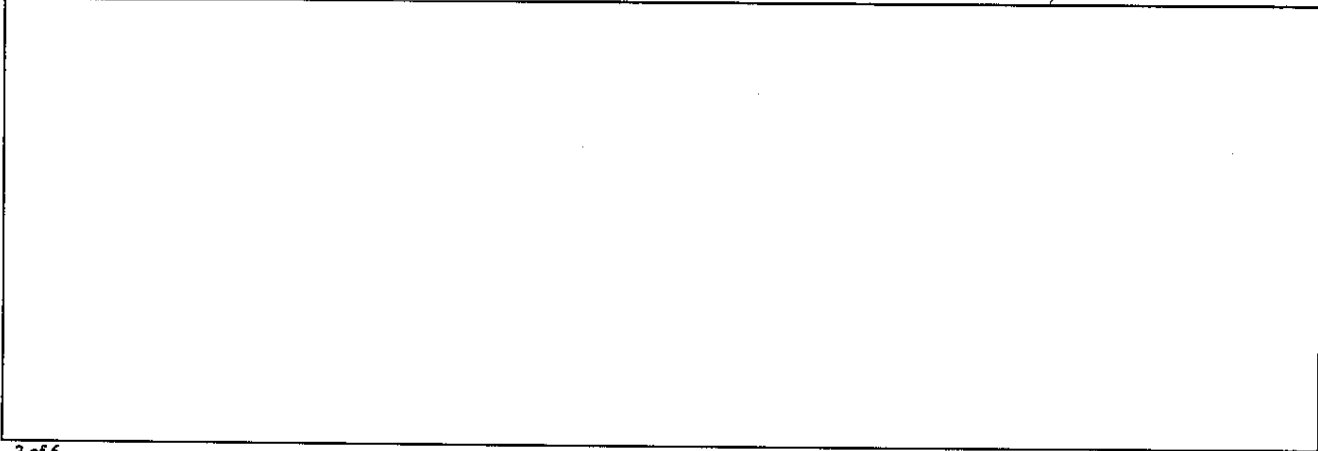
**SECTION 2 - DEFINITIONS**

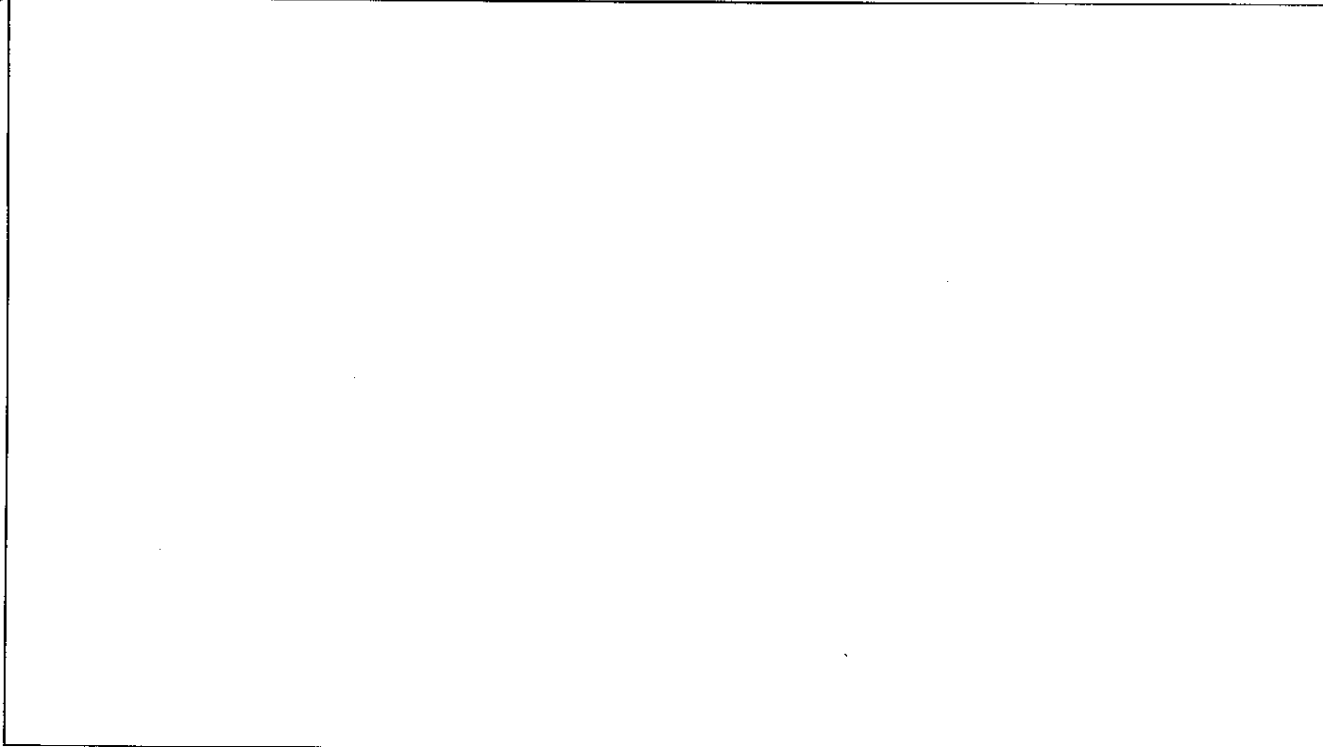
2.1. ~~(S-CCO)~~ The following definitions apply to this Annex only. Unless contradicted or otherwise

supplemented by these definitions, the definitions contained in Section 3 of the basic USSID 18 also apply to this Annex.

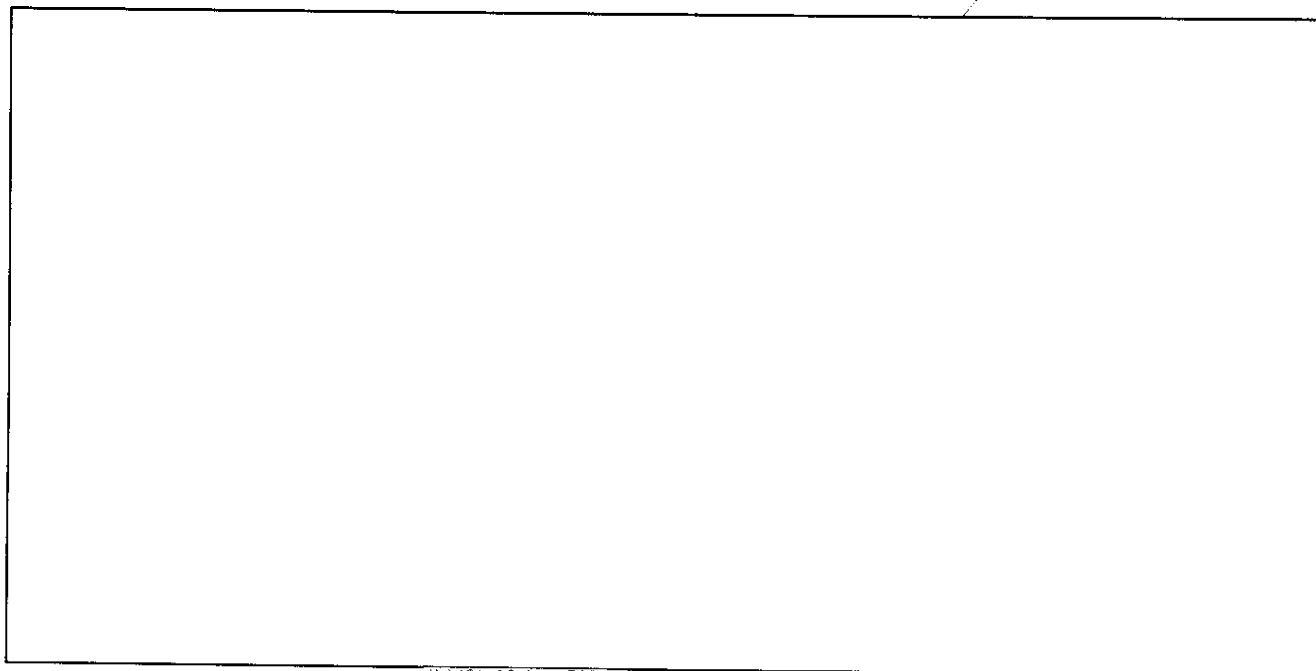


**SECTION 3 - COLLECTION**



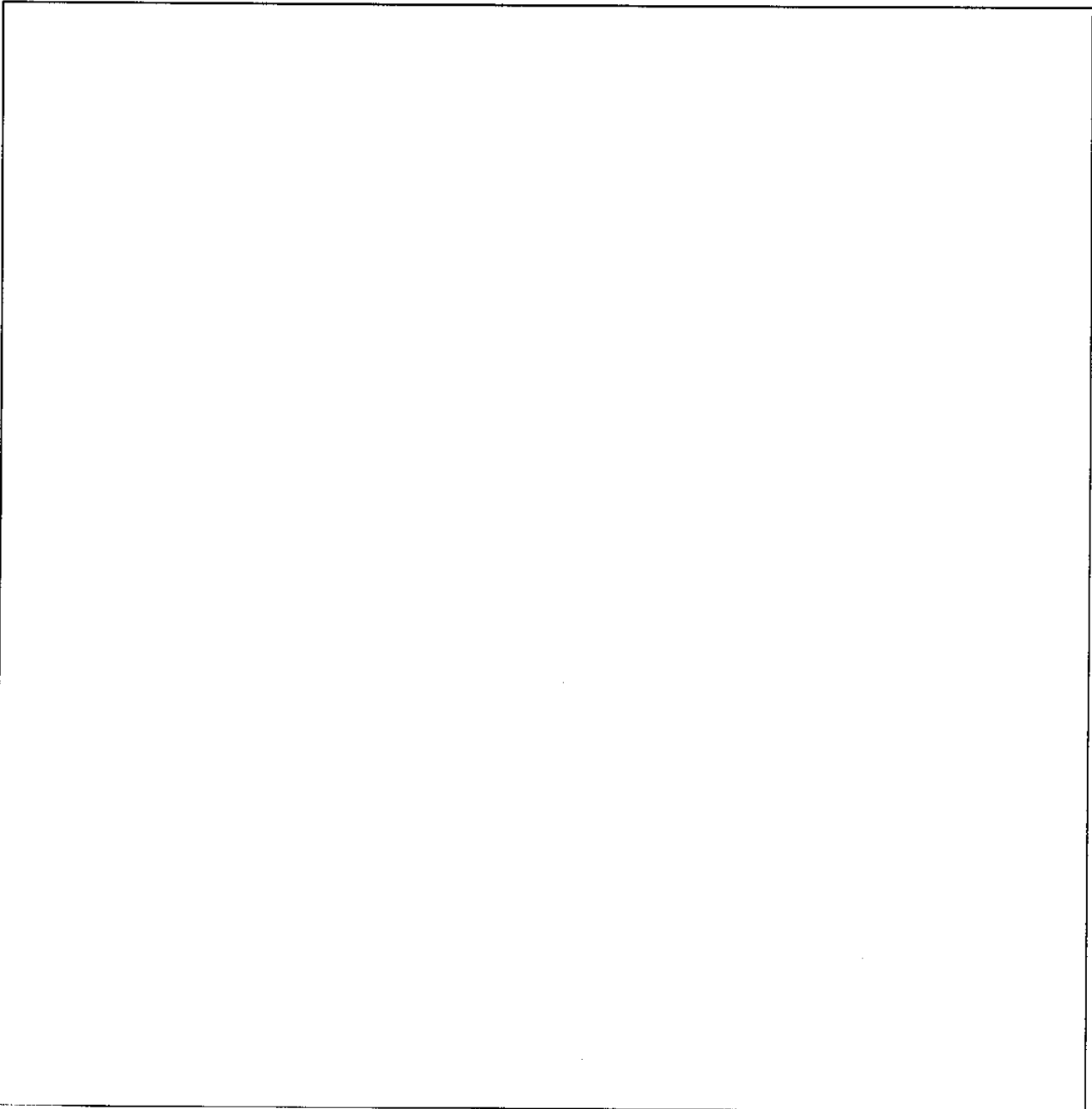


**SECTION 4 - RETENTION**



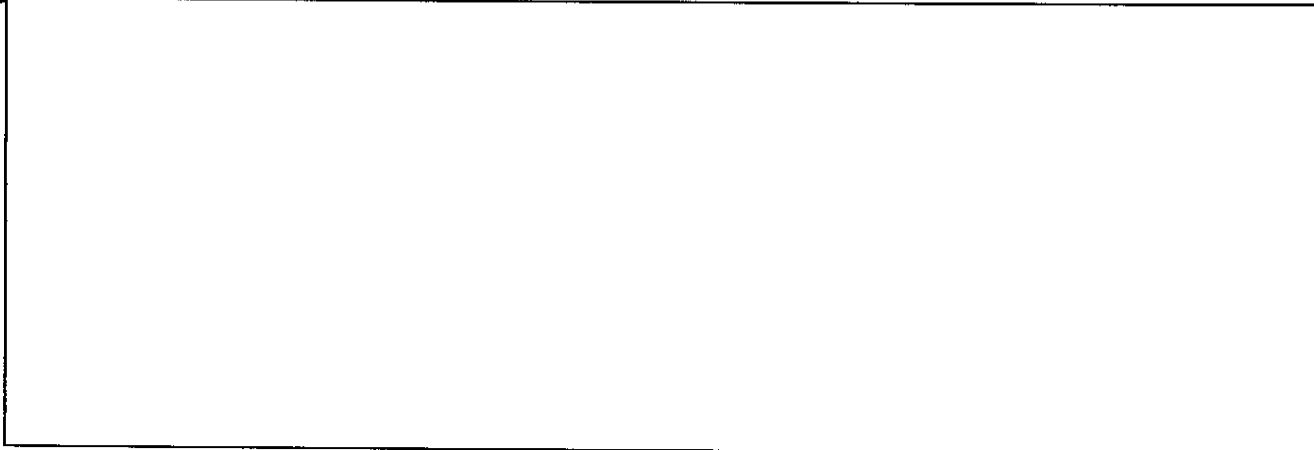
(b) (3)-18 USC 798  
(b) (3)-P.L. 86-36

**SECTION 5 - DESSEMINATION**

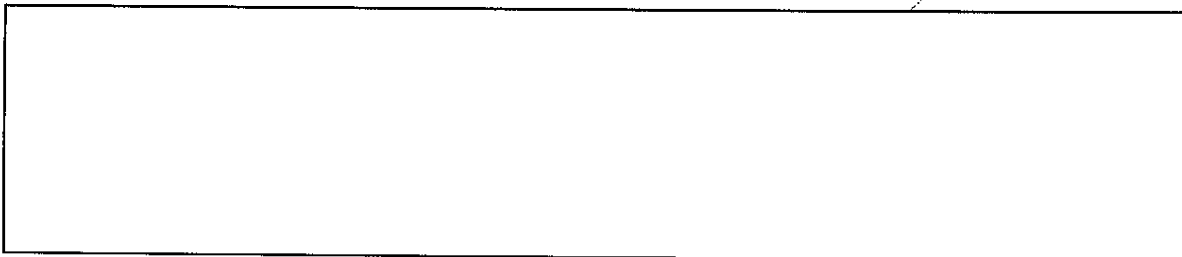


(b) (1)  
(b) (3) - P, T  
(b) (3) - 18  
(b) (3) - 50





**SECTION 6 - IDENTIFICATION OF U.S. PERSONS**



[Return to USSID Index](#)

(b) (1)  
(b) (3) - P.L. 86-36  
(b) (3) - 18 USC 793  
(b) (3) - 50 USC 403

~~SECRET~~

USSID 18  
27 July 1993

ANNEX K

(b) (1)  
(b) (3) - 50 USC 403  
(b) (3) - 18 USC 793  
(b) (3) - P.L. 86-36

[Redacted]  
[Redacted] (~~S-CCO~~)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(~~S-CCO~~)

[Redacted]

[Redacted]

[Redacted]

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

K/1

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~